Appendix Z
Instrumentation, Targets, and Threat Simulators (ITTS)

Section I
Planning and Use

Z–1. Overview

a. ITTS planning and use. This appendix provides general planning guidance for Instrumentation, Targets, and Threat Simulators (ITTS) in support of T&E requirements. It outlines the relationships of key activities involved in planning, managing, and using ITTS in support of test and evaluation, and describes procedures for scheduling and use. The term "ITTS" as used in this appendix includes simulations. Section II prescribes procedures to be followed in the validation and accreditation of threat simulators/simulations and targets. Section III outlines the responsibilities for those organizations associated with the planning, use, and participation in the procedures prescribed by this appendix.

(1) Threat representation and major instrumentation programs are considered Army Acquisition Category (ACAT) III programs. These programs yield complex hardware and/or sophisticated simulation products. They are consequently governed by the same acquisition rules that apply to most Army developments, and are assigned to the Project Manager for Instrumentation, Targets and Threat Simulators (PM ITTS) for programming and execution. Threat representation programs have their own peculiar acquisition planning considerations, but the key to successfully planning and integrating threat representations into testing is the early involvement of PM ITTS, the Army Test and Evaluation Command (ATEC), the System Program Manager (PM) and the Intelligence Community through the T&E Working Integrated Product Team (T&E WIPT).

(2) This appendix describes the planning and use for "common use" and "system specific" threat representations. Common use threat representations are those developed or acquired in support of more than one blue weapon system, whereas system specific threat representations are developed or acquired for only one. PM ITTS funds for common use threat representations by programming their requirements through the Test Budget Operating System (BOS) manager, the Test and Evaluation Management Agency (TEMA). System specific threat representations are funded by the blue weapon system PM through the Equipping Program Evaluation Group (PEG).

(3) Planning for instrumentation and threat representations must occur early in the blue system development process in order to be available for use in support of specific T&E events. Preliminary determinations and related funding estimates must be incorporated both in the Test and Evaluation Master Plan (TEMP) and in the System Evaluation Plan (SEP). This means that test resource planning must be substantially complete prior to Project Management Office (PMO) development of a Cost Analysis Requirements Document (CARD). This also requires that detailed planning be completed prior to ATEC's submission of Outline Test Plans (OTPs) to the Test Schedule and Review Committee (TSARC). Early planning for threat representations and instrumentation is thus key to the successful and timely execution of a testing program.

b. Definition of terms used in this appendix.

(1) *Test instrumentation.* Test instrumentation is a generic term that includes all instrumentation used by testers, to include—

(a) Scientific or technical equipment used to measure, sense, record, transmit, process, or display data during test or examination of materiel.

(b) Simulators, system stimulators, or threat instrumentation used to measure or depict the threat for training, teaching, or proficiency during testing.

(c) Targets used to simulate a battlefield object when destruction of the real object is not practical or the actual object is not available.

(2) *Threat representations.* Threat representations include models, simulations, simulators, emulators, foreign materiel (that is, actual systems), and aerial and ground targets that portray specific foreign military weapon systems or civilian devices used in an adversarial military role. Threat representations are generally grouped in two specific categories—

(a) Threat systems. A threat system is a generic term used to describe simulators, emulators, foreign equipment instrumented for T&E, a model, a simulation federation representing foreign military equipment, or multiple integrated federations. Threat systems portray potential adversary systems and their operation in tactical environments. Simulators and emulators have one or more characteristics that, when detected by human senses or manmade sensors, provide the appearance of an actual foreign system with a prescribed degree of fidelity. When embedded in simulation, validated threat systems portray foreign equipment, its operation, and its tactical employment with high fidelity. This includes signature, communications, performance, lethality, and a host of other factors. Threat systems are generally re-used many times. They are not normally expendable.

(b) Targets. There are three classes of targets. They are- ground, aerial, and virtual. Targets are normally economical, expendable devices used for tracking and/or engagement by missiles/munitions in support of T&E. This factor normally differentiates targets from threat systems. However, targets have other uses. They can, for instance, be utilized multiple times for hyper-spectral data collection in support of research, development, and acquisition. Targets

may be mobile drones controlled by programs or by real-time link. Some targets are not mobile. Ground targets are intended to represent an adversary ground vehicle system or ground based military structure. Aerial targets are intended to represent adversary aircraft or cruise or tactical ballistic missiles. Targets may represent only selected adversary system characteristics or they may faithfully represent all aspects of that equipment. Targets may, in fact, be actual pieces of foreign military equipment not useable or instrumented as a Threat System. Virtual targets provide validated, digitized spectral images of specific foreign military hardware. Digitized structural information representing some foreign military equipment may also be available as virtual target data.

(3) *Major instrumentation, targets, or threat simulators/simulations.* Projects are designated major based on a variety of factors, such as acquisition complexity, assessed relative technical risk, schedule risk, cost, and applicability to other mission areas or services. A project classification decision tree, as well as additional discussion of the design, development, and procurement of such items is discussed in paragraph Z–3.

Z–2. Planning for instrumentation, targets, and threat simulators

a. Planning for specific ITTS to support T&E must begin early in the weapon system Concept and Technology Development phase to ensure timely and adequate support. Requirements identification and documentation for targets and threat simulators/simulations is described in paragraph Z–6, and major instrumentation requirements identification is described in paragraph Z–7. Long-range planning for ITTS follows the process described in paragraph Z–8 of this appendix.

b. When planning for the use of targets and threat simulators, it is important to know how threat information for a United States system is derived and where the information is documented. While these documents are primarily intended to support and justify the development of materiel systems, they are also useful in planning for target and threat simulator/simulation support for the T&E of the system. Such documents include—Operational Requirements Document (ORD), Integrated Program Summary (IPS), Cost and Operational Effectiveness Analysis (COEA), Analysis of Alternatives (AOA), Test and Evaluation Master Plan, System Evaluation Plan (SEP), Outline Test Plan, Threat Test Support Package (Threat TSP), System Threat Assessment Report (STAR), Integrated Threat Tactical Operations Plan (ITTOP), and baseline intelligence products.

c. ITTS acquisition is accomplished through a tailored DOD 5000 series acquisition process by the Project Manager for ITTS. PM ITTS is the Army's single manager for developing and acquiring targets (except training range targets), threat simulators/simulations, and major instrumentation in support of testing. All test activities, PMs, and other materiel developers will coordinate their ITTS requirements with PM ITTS beginning with Concept & Technology Development and continue through the life cycle of the system. It is PM ITTS' responsibility to plan, program, fund, and execute all non-system unique ITTS requirements. It is the responsibility of the PM plan, program, fund and execute all system unique ITTS requirements. Only in those unique cases where PM ITTS cannot provide the ITTS support will the system PM pursue alternate ITTS execution.

Z–3. Needs satisfaction

Major Instrumentation, Targets, and Threat Simulator needs will normally be satisfied from on-hand assets. Satisfaction of needs in excess of on-hand assets should make use of one or more of the following methods, listed in order of preference under major instrumentation and threat representations:

a. Major instrumentation.

(1) Testers are encouraged to survey and query existing inventory databases at ATEC and PM ITTS to determine what resources are available, where they exist, and in what quantities. Direct coordination with designated points of contact (POC) is necessary to ensure availability of their latest data and to gain a complete understanding of an item's capabilities, limitations, support requirements, and suitability, as well as to determine its potential availability. The preferred alternative for meeting instrumentation and test support equipment shortfalls should be through the Inter-range Loan Agreements process. The Range Commander's Council operates a Tri-Service forum for sharing of test support equipment and instrumentation. Refer to the Range Commander's Council Secretariat, ATTN: STEWS–RCC, White Sands Missile Range, NM 88002–8110.

(2) Standard off-the-shelf instrumentation may be leased or rented to satisfy short-term inventory augmentation or one-time needs. A cost benefit analysis should be conducted to compare total lease or rental costs to non-development item (NDI) life cycle (procurement plus ownership) costs over the full instrumentation requirement period before this option is pursued.

(3) Testers may procure standard off-the-shelf NDI instrumentation or modify on-hand inventory assets needed to satisfy test requirements. A trade-off analysis of modification versus procurement of NDI (assuming availability) should be conducted to determine the most cost efficient approach.

(4) Design, development, and procurement of instrumentation should be the exception due to the time and expense associated with such an effort. Experience has shown that the acquisition cycle for non-major instrumentation can easily take 3–5 years and 8–12 years is not uncommon for a major instrumentation system. When development is necessitated, the impact must be closely coordinated through the T&E WIPT and the TSARC, documented, and reflected in the TEMP as a potential test limitation. Figure Z–1 provides an instrumentation project classification decision tree. It should be used as a guideline for determination of major versus non-major ITTS.

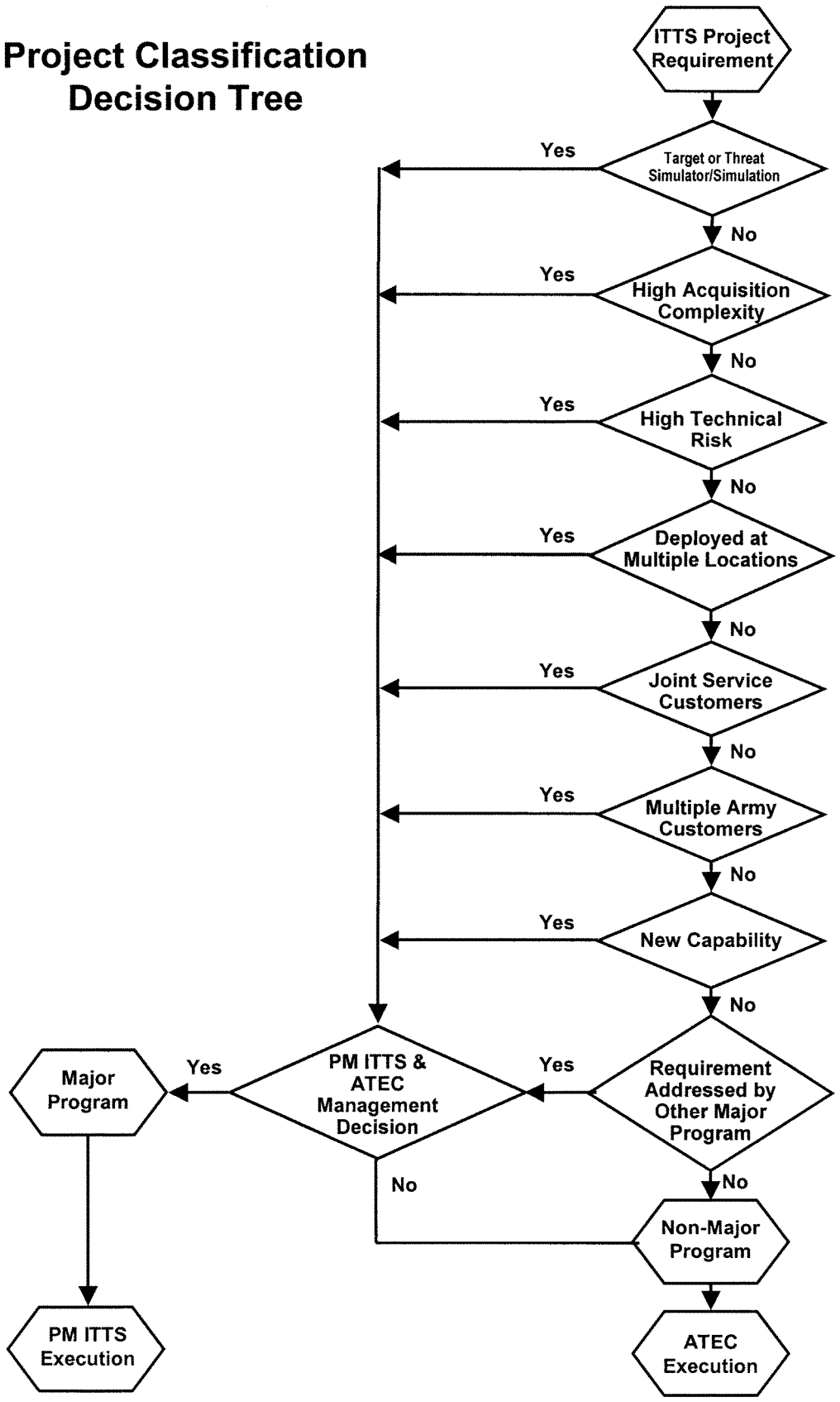

Figure Z–1. Project classification decision tree

b. Threat representations.

(1) Testers are encouraged to query existing inventory databases at PM ITTS as well as other sources such as the Defense Modeling and Simulation Resource Repository (http://www.msrr.dmso.mil) and the Defense Intelligence Modeling and Simulation Resource Repository (https://umsrr.ngic.army.mil) to determine what resources are available, where they exist, and in what quantities. Direct coordination with designated points of contact (POC) is necessary to ensure availability of their latest data and to gain a complete understanding of an item's capabilities, limitations, support requirements, and suitability, as well as to determine its potential availability. The POC for Threat Systems is PM ITTS Threat Systems Management Office, Refer to: Director, Threat Systems Management Office (TSMO), AMSTI–ITTS–S (Operations Team Lead), Bldg 4497, Redstone Arsenal, AL 35898–7461, Telephone (256) 876–9656. The POC for Targets is the PM–ITTS Targets Management Office, AMSTI–ITTS–Q, Redstone Arsenal AL 35898–5798.

(2) Design, development, and procurement of threat representations should be the exception due to the time and expense associated with such an effort. When development is necessitated, the impact must be closely coordinated through the T&E WIPT and the TSARC, documented, and reflected in the TEMP as a potential test limitation. Requirements for developments will be referred to the Threat Systems Integrated Product Team (TS IPT) for prioritization and potential funding.

Z–4. Schedule and use requirements

a. Individual test activities, directorates, ranges, and laboratories possess organic instrumentation assets consistent with their mission focus. Scheduling of organic instrumentation assets is affected in consonance with internal operating procedures. Scheduling of instrumentation assets from external sources is affected by direct coordination between the borrower and lender. Costs associated with instrumentation use are normally limited to those of lease, round trip transportation (if borrowed), and any modifications required for unique or special applications or interface requirements. The latter are typically charged to the customer (that is, the program executive officer (PEO) or PM). Costs should be reflected in the OTP for TSARC approved tests.

b. For TSARC approved tests, requirements for targets will be included within the OTP. Targets developed by PM ITTS are subject to the provisions of validation and accreditation outlined in section II of this appendix. Individual test activities possess limited organic target assets. The vast majority of aerial and ground targets used in support of Army T&E are developed, procured, maintained and operated by the Targets Management Office (TMO). Specific procedural requirements for assets held by other organizations should be coordinated directly with their appropriate POC. Requests for use of assets controlled by TMO will be documented on SMI Form 1209. Refer to Project Manager for Instrumentation, Targets, and Threat Simulators, ATTN: AMCPM–ITTS–Q, Redstone Arsenal, AL 35898–5798.

c. For TSARC approved tests, requirements for threat simulators/simulations will be coordinated with TSMO and included within the OTP. Specific procedural requirements for assets held by other organizations should be coordinated directly with their appropriate POC. Scheduling of TSMO assets is accomplished through direct coordination with them and should be affected no later than 24 months in advance of the required test date. Formal schedule coordination and approval for use is conducted as a part of the TSARC process. For all types of test and training support, TSMO will prepare a cost estimate for use in communication and coordination with the customer. For TSARC approved tests, costs associated with threat simulator support will be included within the OTP.

Z–5. Associated data for planning and use of ITTS

In addition to the system documentation and reports mentioned in the preceding paragraphs, additional databases and inventories are available for reference when planning and scheduling the use of instrumentation, targets, and threat simulators. Some of these include the following:

a. Test facilities. ATEC HQ Instrumentation Division manages a database as a tool to identify existing Army major test facilities, major instrumentation, and test equipment. The database identifies assets by location, value, capability, and points of contacts to provide the test community with a readily available list of assets. Narrative descriptions and performance information identify system-unique capabilities of the facilities listed, while a list of major projects and programs supported enables identification of any similar or related uses that have already employed the facility. Refer to Commander U.S. Army Test and Evaluation Command, CSTE–OP–IN, 4501 Ford Ave., Alexandria, VA 22302–1458.

b. Automated Joint Threat Systems Handbook (AJTSH). The Automated Joint Threat Systems Handbook (AJTSH) is a stand-alone information retrieval database used for mission planning of joint and single Service exercises and preliminary planning of test projects. It provides user information on threat representative simulators, targets, actuals, models and simulations and related test ranges. Users are able to search for one or more test and/or training assets, associated technical data, and points of contact for additional information and scheduling. It is available on CD-ROM for stand alone operation and can also be accessed via SIPRNET. For additional information, contact the Threat Systems Office, Director, Operational Test and Evaluation (DOT&E).

c. ATEC Instrumentation Development and Acquisition Program (IDAP). The ATEC Instrumentation Development and Acquisition Program (IDAP) is an automated instrumentation requirements database that incorporates instrumentation requirements for ATEC HQ and its subordinate commands. The database is used to outline current and long range instrumentation requirements, funding and schedule requirements, and life cycle planning. Refer to Commander U.S. Army Test and Evaluation Command, CSTE–OP–IN, 4501 Ford Ave., Alexandria, VA 22302–1458.

d. Facilities and Capability Information for Test and Training (FACITT). Facilities and Capability Information for Test and Training (FACITT) is a Web-based information search tool created to satisfy the DOD requirement for locating both DOD and non-DOD facilities and capabilities that could perform test and training activities. Leveraging off the existing Web sites at these facilities, FACITT locates the facility and capability information through a focused Web-crawl and cataloging process. FACITT also includes linkable maps and catalogs that permit the user to link directly to the related sites. FACITT can be accessed at http://jcs.mil/.

e. Targets Information Manual. This manual serves as a descriptive catalog of Army targets and foreign ground assets available (or in development) for support of T&E or training. Refer to Project Manager for Instrumentation, Targets, and Threat Simulators, ATTN: AMCPM–ITTS–Q, Redstone Arsenal, AL 35898–5798.

f. Threat Systems Management Office (TSMO) Threat Inventory Database. PM–ITTS/TSMO maintains a database of all available assets for both hardware simulators and software simulation systems. These assets are available for use in testing and training. Refer to Project Manager for Instrumentation, Targets and Threat Simulators at: Director, Threat Systems Management Office, AMSTI–ITTS–S (Operations Team Lead), Bldg 4497, Redstone Arsenal, AL 35898–7461, Telephone (256) 876–9656.

Z–6. Threat requirements generation process for targets and threat simulators

This paragraph describes and figure Z–2 illustrates, in general terms, the process of identifying, coordinating, and prioritizing threat requirements in support of test and evaluation. The objective of the process is to identify and prioritize those threats that must be replicated in the form of a target, threat simulator, or threat simulation in order to support test and evaluation. The product of the process is a coordinated and prioritized list of requirements that can be considered for funding through the Planning, Programming, Budgeting, and Execution System process.

a. The process is initiated with the conduct of Mission Area Analyses (MAA). MAAs are conducted at each Intelligence Production Center (IPC), where Science and Technical Intelligence (S&TI) is melded with General Military Intelligence (GMI) to identify general threat trends and developments.

b. The next step in the process is primarily an intelligence-initiated series of threat conferences (see AR 381–11) to address more specific threats as they pertain to functional areas. Participants in this portion of the process include representatives from one or more IPCs, the Defense Intelligence Agency (DIA), appropriate PMs, the Training and Doctrine Command (TRADOC), PM ITTS, and testers. The product of these conferences is a series of validated threat descriptions that U.S. Army weapon systems may encounter on the battlefield. Test specific threat items, however, are not identified during these conferences. The products of these conferences feed the STAR development process and are made available to the Research Development & Engineering Centers for the establishment of Science and Technology Objectives.

c. Another user of the threat conferences' product is the T&E WIPT. The T&E WIPT acts as a filter to refine the output from the conferences into test specific threats that will support the data collection requirements of individual tests. It is the responsibility of the T&E WIPT with guidance from the Threat Intelligence Community, to define the threats to be represented, the level of fidelity of the representations, and the environments in which the threat representations will need to operate (such as. open-air range, simulation, or within a specific architecture). This product of the T&E WIPT is input to the Threat System-Integrated Product Team (TS IPT) requirements prioritization process and forms the basis of a "contract" between the tester and the PM as to the threats that will be used in testing. The T&E WIPT integrates these threat representations into an appropriate integrated testing strategy that is reflected in the System Evaluation Plan (SEP) and the TEMP. The Threat Systems Management Office (TSMO) representatives to the T&E WIPT identifies existing threat resources that could be applied to the program and highlights shortfalls in threat resources. Shortfalls that are applicable to more than one development are reported to the TS IPT for budgeting and execution planning. Substantive threat issues that cannot be resolved by the T&E WIPT will be elevated through channels to the appropriate Threat Coordinating Group for resolution. If resolution is not achieved, the issues will be elevated to the program's Overarching IPT.

d. Following the filtering process by the T&E WIPT, the TS IPT prioritizes the threat requirements. This prioritization is reflected in the Army Threat Systems Master Plan (ATSMP), a document reflecting coordinated and prioritized threat requirements necessary to support the testing, training, and PM communities. The ATSMP is prioritized jointly by ATEC and PM–ITTS and provided to TEMA for budgeting and programming consideration at Headquarters, Department of the Army. In the same manner, the ATSMP will also document system specific threat requirements in support of testing for individual PMs identified through the T&E WIPT for Army visibility and planning.

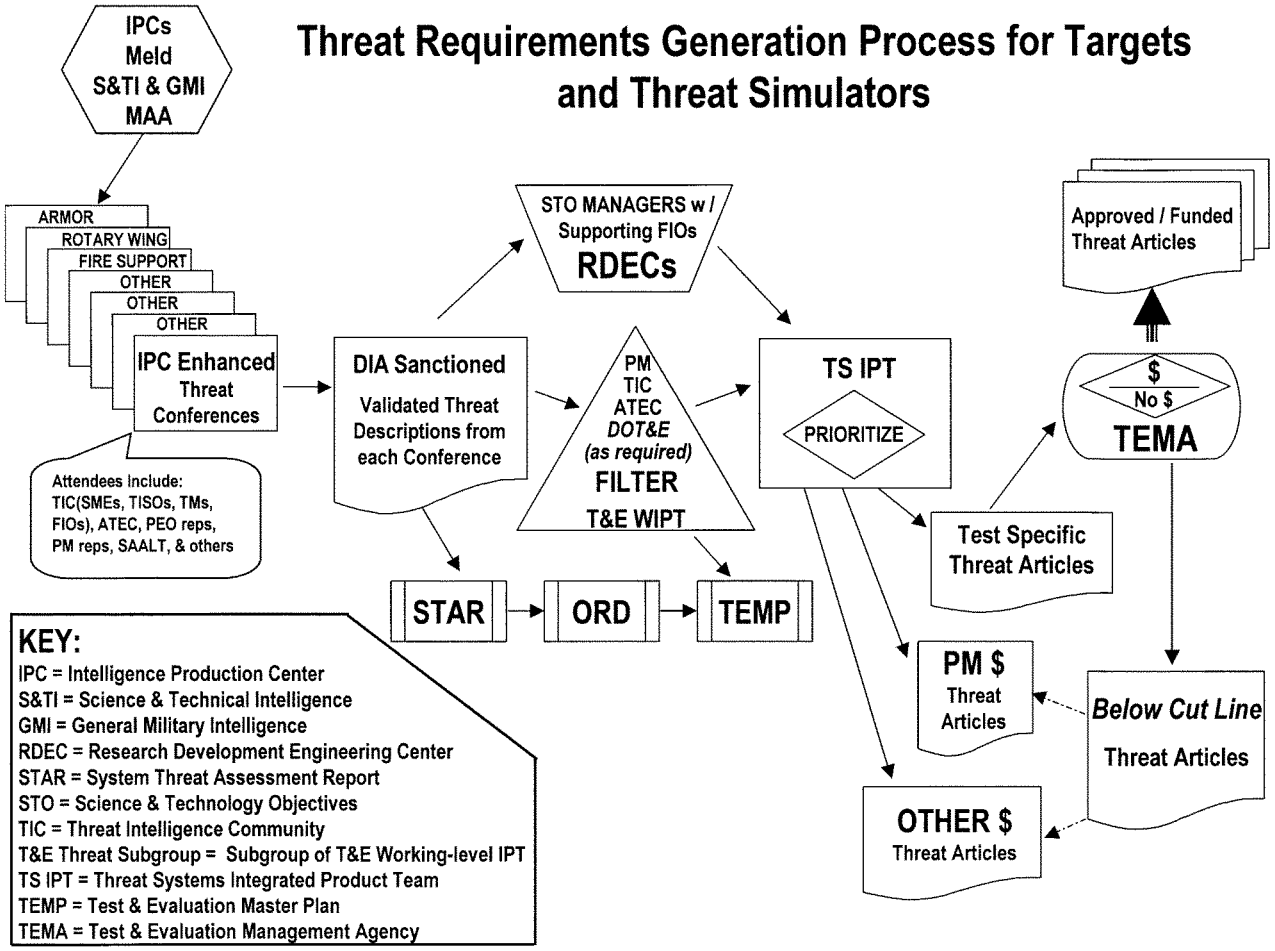

Figure Z–2. Threat requirements generation process for targets and threat simulators

Z–7. Major instrumentation requirements generation process

The process discussed in this paragraph provides general information for the user who is unable to fulfill instrumentation needs from inventory.

a. Each step of the major instrumentation requirements process is accompanied by the documents, actions and approvals required from the identification of a need by a user to the initiation of a project. The process and documentation requirements should be tailored based on agreement between the user and materiel developer. For all major instrumentation, the following are required:

(1) Formation of an Instrumentation Working Group (IWG).

(2) Approval of documented requirements by a designated officer/civilian representing the user.

(3) Acceptance of the documented requirements by a designated officer/civilian representing, PM ITTS, the MATDEV.

(4) A joint agreement signed by both the user and PM ITTS that outlines the developer's approach, schedule and cost estimate.

b. The user (such as, HQ ATEC, a Materiel Development Command, PEO or PM) generates a requirement based on a need that is validated through documented references. These references may be the Army Science and Technology Master Plan (ASTMP), the Five Year Test Program (FYTP), T&E WIPT minutes, the system TEMP, the Army Test Resources Master Plan (ATRMP) or any other such official document. The long range planning process described below provides the methodology used for identifying and refining requirements in the ASTMP. ATEC HQ and the U.S. Army Space and Missile Defense Command (SMDC) will also identify needs to enhance their respective test facility

infrastructure, improve testing efficiency, and improve operational safety. These needs will be documented by each command.

c. The user then reviews all requirements, checks for unwarranted duplication, and confirms adherence to the command long-range plan and the ATRMP. The user then performs the following functions—

(1) Prioritization of requirements.

(2) In conjunction with PM ITTS, identifies major instrumentation projects for management and execution in accordance with figure Z–1. Procedures specific to the interaction between ATEC, USASMDC, and PM ITTS can be found in section III, paragraph Z–13 (Instrumentation Requirements). Development programs not managed by PM ITTS will be internally managed by the user and are not addressed in this appendix.

d. For major instrumentation, PM ITTS and the user will form and jointly chair an Instrumentation Working Group (IWG). The IWG will operate during the preparation and staffing of the documented requirements. The functions will be to mutually understand the requirements and establish general project milestones and documentation requirements.

e. The ITTS user will lead in preparing the documented requirements. PM ITTS and the U.S. Army PEO Simulation, Training, and Instrumentation Command (PEO STRI) will provide support as determined by the IWG. All documented requirements will be staffed within the using command and PM ITTS. The using commander (or designee), the test agency, PEO, or weapon system PM will approve and sign the documented requirements. A designated officer/civilian from PEO STRI will also sign the document as the MATDEV indicating the acceptance of the project and understanding of the requirement. The requirement documentation will be forwarded to TEMA.

f. The IWG will coordinate activities during the Concept Exploration phase. PM ITTS will study tradeoffs and prepare acquisition documents as required by the IWG. Trade-off studies may be performed as directed by the IWG. The user should select the best technical approach based upon projected resources and technical requirements. Both the user and PM ITTS will agree upon a development approach, schedule and cost estimate to satisfy the requirement. This agreement will be documented and jointly signed by the using commander (or designee), test agency, PEO, and a PM ITTS designee. The agreement will be forwarded to TEMA.

g. Joint Service reviews are required in the following instances:

(1) Projects competing for OSD test and evaluation funds, are reviewed by tri-Service Reliance panels, comprised of subject matter experts organized by test capability areas. The results of these reviews are forwarded through the Test and Evaluation Executive Agent structure for funding consideration as part of the Central Test and Evaluation Investment Program (CTEIP).

(2) CTEIP projects that are for short-term OT&E requirements only, are reviewed by the OSD Test Investment Coordinating Committee (OTICC). The OTICC reviews all Services' OT&E requirements for unwarranted duplication and recommends a joint Service prioritized list of "needs and solutions" to OSD for funding consideration. As a result, potential OSD funded candidates and multi-Service duplications are identified.

Z–8. Long-range planning for ITTS

TEMA will survey on an annual basis the technology capabilities of Army test and evaluation facilities. The purpose of the survey will be to ascertain where future improvement and modernization investments should be made. The information resulting from the survey will be used to provide Army Program Objective Memorandum (POM) guidance and will be published as part of the annual ATRMP. The concept of the survey is evolving. The first survey was completed in the Fall of 2001 and published as part of the 2002 ATRMP, providing guidance for the FY 04–09 POM build. The first survey was conducted by gathering subject matter experts from test technology areas resulting in a series of roadmaps depicting required investments needed to maintain pace with emerging technologies and weapon systems development. Future surveys may follow a similar format or evolve into a different structure. Regardless of format, the objective will be the same; to roadmap the major improvement and modernization investments needed for test and evaluation. In preparation for the annual survey, all commands involved with test and evaluation should continuously review and update the T&E technology roadmaps published in the ATRMP.

Section II
Validation and Accreditation Procedures for Threat Simulators and Targets

Z–9. Overview of validation and accreditation procedures

a. This section provides the procedures used by the Army Validation and Accreditation Program for Threat Simulators and Targets. The processes, concepts, and procedures employed in validation and accreditation of targets and threat simulators are defined and prescribed. The roles and responsibilities of the Department of the Army agencies and organizations involved in validation and accreditation are identified in section III, paragraphs Z–14 and Z–15 respectively. These procedures implement and support DOD Threat Simulator Program Guidelines, chapter 3 of the Defense Acquisition Guidebook, concerning threat simulators/simulations and targets, and are issued in compliance with AR 73–1, DA Pam 73–1, and AR 381–11. Threat simulation, validation, and accreditation procedures can be found in AR 5–11 and DA Pam 5–11. Additional software-specific validation guidelines for submitting threat

simulation validation reports for use in support of T&E are currently undergoing development and will be published as interim policy guidance until the next publication of this pamphlet.

b. These procedures are applicable to Army threat simulators/simulations and targets, which represent a part or function of a specific threat system, and will be used in tests supporting milestone decisions. Exceptions to the validation process will be addressed on an individual basis. All requests for exceptions should be forwarded to the Director, U.S. Army Test and Evaluation Management Agency, 200 Army Pentagon (ATTN: DACS–TE), Washington, DC 20310–0200. A validation waiver, used to facilitate accreditation, does not preclude system validation requirements. Accreditation waivers are not granted.

c. Figure Z–3 illustrates the generic relationship of validation and accreditation support to the life cycles of Army materiel development and threat simulators/simulations and targets. As shown in the figure Z–4, validation is performed at critical points throughout the life cycle of threat simulators/simulations and targets. Accreditation pertains to specific test applications of threat simulators and targets during the operational phase of their life cycle. Validation Working Groups (VWGs) accomplish validations through a series of periodic meetings. The effectiveness of each VWG is entirely dependent on the ability of its membership to address a validation event for a given target, simulation or simulator. Validation must not be viewed as an evaluation where the relative worth of a system is being graded; it is a process for comparing simulators/simulations and targets to DIA-approved threat data, documenting the variations, and assessing the impact of those differences on the potential use of the simulator, simulation or target. The VWG task is finished: when the VWG members sign the completed Validation Report (VR); the report is forwarded to and approved by the Director, TEMA and, as required, forwarded to and approved by the Director, Operational Test and Evaluation (DOT&E).

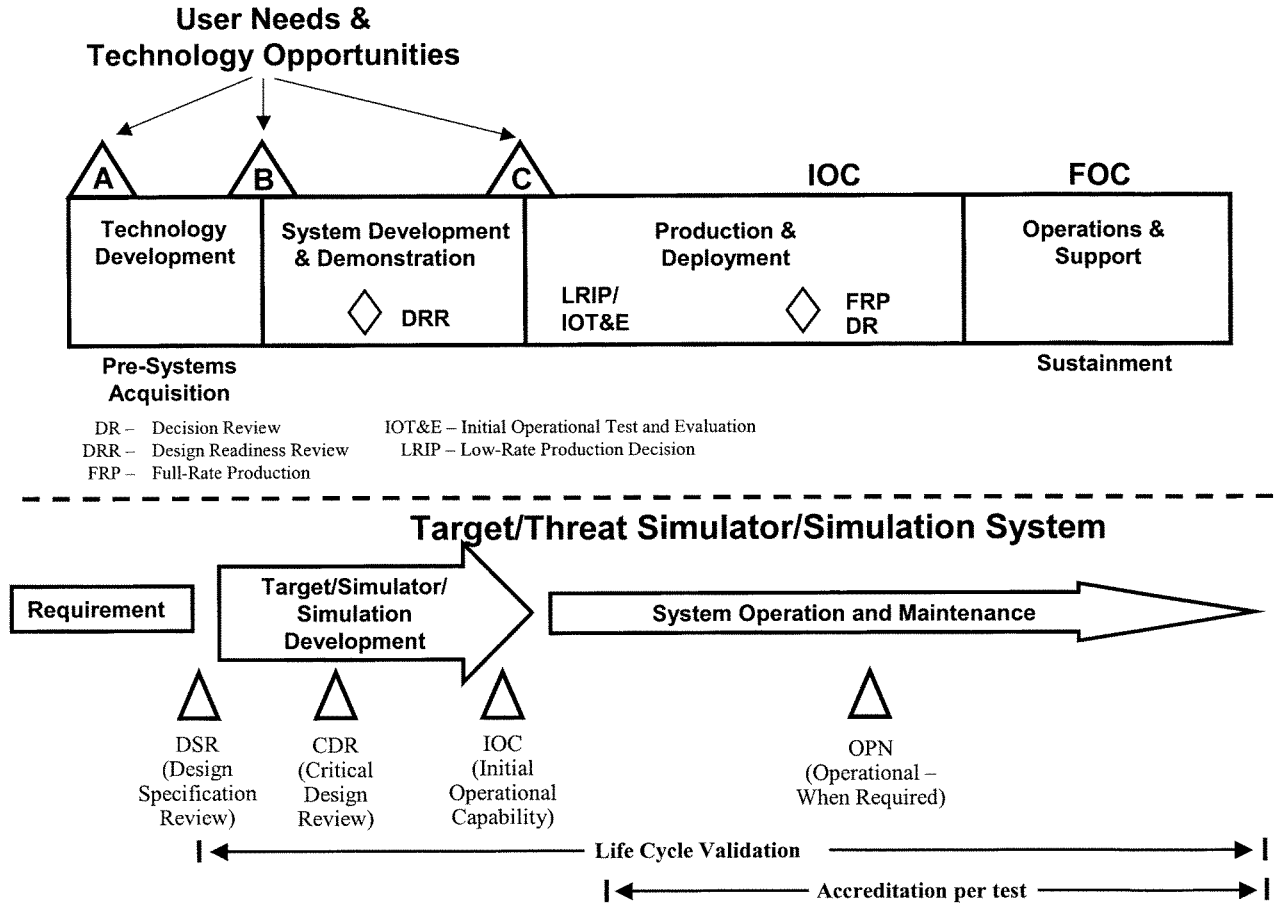

Figure Z–3. Validation/accreditation support to the DOD life cycle model

Z–10. Validation of threat simulators/simulations

a. Validation is the process used to document and analyze critical performance differences a threat simulator/simulation may demonstrate when compared with DIA-approved data. Threat simulators/simulations are developed to portray actual threat system visual likeness and performance capability for user-identified test and training requirements. Accordingly, threat simulators/simulations may only duplicate or represent a limited number of threat system attributes. Therefore, threat system validation must be based upon expert knowledge of the threat, the simulator/simulation, and user requirements. A VR will be issued documenting specifics of the validation effort. Due to the differences in the validation of hardware (simulators) and software (simulations), the content of the respective VR will differ slightly as provided in the validation report content instructions in table Z–1. Responsibility for funding developmental validation costs belongs to the threat simulator or target MATDEV. Periodic operational validation costs will be funded by the owning organization.

Table Z–1
Validation report format and content

Threat Simulator/Target Validation Report format	Threat Simulation Validation Report format
Table of Contents	**Table of Contents**
EXECUTIVE SUMMARY This section is the last section written and is a condensed version of sections I through VI. The major elements of the six sections should be covered. No material is provided here that is not provided in the other six sections in greater detail. Much of the detailed discussion is not included here but is found only in the main body of the report. This section should be two to three pages in length, unless there are a large number of differences and impacts to address. This should be a standalone section.	**EXECUTIVE SUMMARY** This section is the last section written and is a condensed version of sections I through VI. The major elements of the six sections should be covered. No material is provided here that is not provided in the other six sections in greater detail. Much of the detailed discussion is not included here but is found only in the main body of the report. This section should be two to three pages in length, unless there are a large number of differences and impacts to address. This should be a standalone section.
SECTION I INTRODUCTION 1. Purpose 2. Threat Representation 3. Points of Contact This section should briefly state what threat this simulator/target is expected to represent, what portion of the threat is included, what is left out, and the relationship of this simulator/target to others if it is a portion of a larger system, or a modification of a larger system. It also should state whether the simulator/target is expected to represent multiple variants of the threat, if such variants exist. The purpose or objective of the validation report should be stated. This section should also include a statement that the validation report describes the status of the simulator/target's ability to emulate the threat at that point in time, and that there may have been changes in the threat definition or in the simulator/target since the validation report was written. The introduction should identify a point of contact for users to gain additional information.	**SECTION I INTRODUCTION** 1. Purpose 2. Threat Representation 3. Points of Contact This section should briefly state what threat this simulation is expected to represent, what portion of the threat is included, what is left out, and the relationship of this simulation to others if it is a portion of a larger simulation or a modification of a larger simulation. It also should state whether the simulation is represents multiple variants of the threat, if such variants exist. The purpose or objective of the validation report should be stated. This section should also include a statement that the validation report describes the status of the simulation's ability to emulate the threat at that point in time, and that there may have been changes in the threat definition or in the simulation since the validation report was written. The introduction should identify a point of contact for users to gain additional information.
SECTION II VALIDATION PROCEDURES This section should identify the directives that apply to this report. It should identify the sources of data for both the threat and the simulator/target, along with the process used in determining the impacts of differences between the threat and the simulator/target that have been documented.	**SECTION II VALIDATION PROCEDURES** This section should identify the directives that apply to this report. It should identify the sources of data for both the threat and the simulation, along with the process used in determining the impacts of any differences between the threat and the simulation or any limitations of the simulation that have been documented. In addition, it should describe the assumptions, constraints, methods employed, data, tools, and techniques used to conduct the validation.
SECTION III THREAT DESCRIPTION This section should provide a brief narrative description of the threat as it is currently defined. It should also state that the data have been extracted from DIA documents or identify the other documents used as source data for the threat information. State if the DIA has approved any or all of the data that were drawn from non-DIA documents. Generally, block diagrams should be placed in appendix A rather than in this section. Operational doctrine, time sequence from Acquisition to Track to Launch to Intercept, type of system, for example, are appropriate in this section. Discussion that builds on the data provided in appendix A or provides additional explanation of the information in appendix A should be included.	**SECTION III THREAT DESCRIPTION** This section should provide a brief narrative description of the threat as it is currently defined. It should also state that the data have been extracted from DIA documents or products or identify the other documents or products used as source data for the threat information. State if the DIA has approved any or all of the data that were drawn from non-DIA documents or products. Operational doctrine, event sequences, and type(s) of system(s), for example, are appropriate in this section. Discussion that builds on the data provided in appendix A or provides additional explanation of the information in appendix A should be included.

Table Z–1
Validation report format and content—Continued

Threat Simulator/Target Validation Report format	Threat Simulation Validation Report format
SECTION IV SIMULATOR/TARGET DESCRIPTION This section should specifically identify all the functions of the threat that are included, and any of the functions of the threat system that are not included as part of the simulator/target. If some portions are simulated in hardware (for example, target tracker and missile seeker), while other portions are simulated in software (for example, missile fly-out), that too should be stated. It is preferred that a simulator/target system be fully addressed in one report, rather than breaking it apart into two or more reports (for example, the target tracker in one report, with the missile seeker and the fly-out model in a separate report). In many cases the simulator/target is programmable in a number of areas and could be readily changed as the threat definition changes. Significant programmability should be covered in this section. As it is also important that the programmable features cover the current threat estimate, the report should include that information. If there are any special modes of operation they should be described here.	**SECTION IV SIMULATION DESCRIPTION** This section should specifically identify all the functions of the threat that are included, and any of the functions of the threat system that are not included as part of the simulation. It should also describe the overall capabilities and typical uses of the simulation, the functional capabilities represented (system, behaviors, environment, and phenomenon), and the level of fidelity at which each function or object is represented. This section should also address the assumptions upon which the simulation was developed as well as assumptions pertaining to user inputs and model-generated outputs. A brief history of the simulation development and any previous validations conducted should be included. Finally, this section should describe the degree to which the software is free from error, the appropriateness and error-freeness of the data as well as any transformations used to convert the data from one format to another, and the degree to which the simulation output agrees with real world objects. For the purposes of threat simulation validations, "real world" objects may include results of other standard or generally accepted simulations (benchmarking), subject matter expert review, face validation, and comparison with test data or foreign materiel exploitation data.
SECTION V DISCUSSION OF DIFFERENCES AND IMPACTS This section should address all the significant impacts on testing or training that may occur due to differences between the current threat and the simulator/target. These statements of impacts may be based on a single difference between the threat and the simulator/target, or they could be based upon a group of differences. If there are differences that tend to counter-balance the impact each may have individually, they should be discussed together. There is no need to address each difference between the threat and the simulator/target, only those that individually or collectively could be expected to have an impact on test or training results. While specific systems that have been designated to be tested against the simulator/target can be useful in identifying some of the impacts of differences, the VWG should consider all types of systems that may undergo testing with this simulator//target when they identify the impacts of differences.	**SECTION V DISCUSSIONS OF DIFFERENCES AND LIMITATIONS AND THEIR IMPACTS** This section should address all the significant impacts on testing or training that may occur due to differences between the current threat and the simulation or limitations of the simulation. These statements of impacts may be based on a single difference between the threat and the simulation of they could be based upon a group of differences, or on a single limitation or multiple limitations. This section should address limitations and conditions of applicability of the simulation to include any intentional and unforeseen limitation, limitations resulting from known but uncorrected errors, and limitations pertaining to user inputs and model generated outputs. Key to this section is a statement of the usability of the simulation for the specific systems that have been designated to be tested against the simulation as well as other types of systems that may undergo testing with this simulation.
SECTION VI CONCLUSIONS AND RECOMMENDATIONS This section should address the overall conclusions and recommendations that can be reached on the basis of the impacts of the differences between the current threat and the simulator/target. There may be several impacts that affect only one type of test, leaving the simulator/target well suited for other tests. This should be stated. It is possible that the simulator/target is so different from the threat in one or several different areas that a modification is recommended.	**SECTION VI CONCLUSIONS AND RECOMMENDATIONS** This section should address the overall conclusions and recommendations that can be reached on the basis of the impacts of the differences between the current threat and the simulation or on the limitations of the simulation. There may be several impacts that affect only one type of test, leaving the simulation well suited for other tests. This should be stated. It is possible that the simulation is so different from the threat in one or several different areas that a modification is recommended. This section should also describe any implications for simulation use.
SECTION VII REFERENCES This section should list all references used in the report.	**SECTION VII REFERENCES** This section should list all references used in the report.
APPENDIX A Section A1. This section should provide a key to the abbreviations used in the data entries in section A2. All the items such as NA or N/A, Nap, NSm, should be explained. Whenever the threat data has no confidence level associated with it, the report should state how data in the Confidence Level column have been coded to show that fact. Section A2. This section should contain the Standard Validation Criteria (SVC) from the appropriate appendix/annex of the DOD Threat Simulator Program Plan with all the threat simulator/target data. In cases where the simulator/target has been made programmable, do not simply state programmable. The range of programmability must be stated along with the fact that the function is programmable. If any of the programmable items have been	**APPENDIX A** Section A1. This section should provide a summary table identifying the significant entities represented in the simulation, the function of each, an indicator of the level of confidence in the representation of that entity and function and any comments. Section A2. This section should include a representative sample of the results of tests or comparisons performed as part of the simulation validation effort and as described in the simulation validation plan. Tests or comparisons that illustrate simulation errors, limitations or differences from the threat should be included as well. In most cases, these results will appear as graphs. Section A3. This section, when applicable, should contain the Standard Validation Criteria (SVC) from the appropriate appendix/annex of the DOD Threat Simulator Program Plan with all the threat

Table Z–1
Validation report format and content—Continued

Threat Simulator/Target Validation Report format	Threat Simulation Validation Report format
programmed such that they do not match the current threat definition, this must also be stated. Validators' notes and threat analysts' comments should be identified in the Remarks column, and included at the end of this section. All portions of the SVC should be addressed, however for those portions that do not apply, such as Continuous Wave parameters for a pulsed radar system, simply state "Not Applicable" for the header entry for that group of parameters and delete subordinate parameter numbers and names in the group from the report. The threat analyst should already have accomplished this. Do not leave out a portion of the SVC without explanation.	simulator/target data. In cases where the simulator/target has been made programmable, do not simply state programmable. The range of programmability must be stated along with the fact that the function is programmable. If any of the programmable items have been programmed such that they do not match the current threat definition, this must also be stated. Validators' notes and threat analysts' comments should be identified in the Remarks column, and included at the end of this section. All portions of the SVC should be addressed, however for those portions that do not apply, such as Continuous Wave parameters for a pulsed radar system, simply state "Not Applicable" for the header entry for that group of parameters and delete subordinate parameter numbers and names in the group from the report. The threat analyst should already have accomplished this. Do not leave out a portion of the SVC without explanation.

(1) A Test Support Package (TSP) contains the narrative, pictorial, and parametric description of the threat system being simulated. It is provided by the MATDEV and approved by the appropriate IPC. Standard formats and parameter listings prepared by the former CROSSBOW committee (now identified as the Threat Simulator Investment Working Group (TSIWG)) are used as guides. The TSP contains the most current information available concerning the threat system; this information is required for section III of the VR.

(2) The System Description (SD) contains the narrative, pictorial, and parametric description of the simulator/simulation undergoing validation. The simulator/simulation developer using the same format and parameters as the TSP prepares it. Depending on the stage of simulator/simulation development, the SD contains either the most current design specifications or actual measured data from the threat system being validated. This information is necessary for section IV of the VR.

b. In order for validation requirements to comply with DOD Guidelines, validation must be accomplished throughout the threat simulator/simulation life cycle. Figure Z–4 depicts the validation events in the threat simulator life cycle.

(1) Validation of the design specification, called a Design Specification Review (DSR), establishes a means for the evaluation of the threat simulator/simulation design, the current DIA approved intelligence regarding the threat system, the projected use of the device or simulation and the simulation validation plan. Appendix F of DA Pam 5–11 provides a sample validation plan format. The completion of a DSR VR is required but is not reviewed by HQDA. The threat system developer, however, is required to submit a memorandum to TEMA stating that the DSR process has been completed and coordinated with the relevant integrated process team. The results of the DSR process will be highlighted indicating, as a minimum, that the threat system developer, the appropriate IPC, and the intended customer concur with the design of the simulator/simulation and the decision to proceed beyond the design phase. Nonconcurrences must be explained in the memorandum. General validation procedures are followed when conducting a DSR, however, no actual measurements are taken at this stage of development since there are only design specifications and intelligence data to evaluate. Every effort must be made to complete a DSR prior to proceeding beyond the design phase. Should an Initial Operational Capability contract be awarded prior to completion of DSR, only minimum expenditure of program dollars may be authorized, and a copy of such authorization from the Materiel Decision Authority (MDA) must be furnished to TEMA documenting the decision and circumstances pertaining thereto.

(2) Validation at Initial Operational Capability (IOC) provides the first opportunity to compare the complete, functional threat simulator/simulation, current DIA approved intelligence estimates of the threat system, and the operational requirement for the device or software. This validation is used to support the fielding decision and documents the performance of the threat system/simulation for test planning and audit purposes. TEMA and as appropriate DOT&E, approval of the VR is required prior to simulator/simulation use in testing and where resulting data will be used in a report or otherwise to support a milestone decision by the appropriate MDA. The IOC validation is the final validation prior to fielding the system/simulation; therefore, it is based on actual measurements (simulators) or data generation (simulation) and the most recent intelligence data. IOC is the most complete and thorough validation a system/simulation will undergo since it is essential at this point to confirm and define the differences between actual measured simulator data or simulation-generated data and the DIA approved threat data.

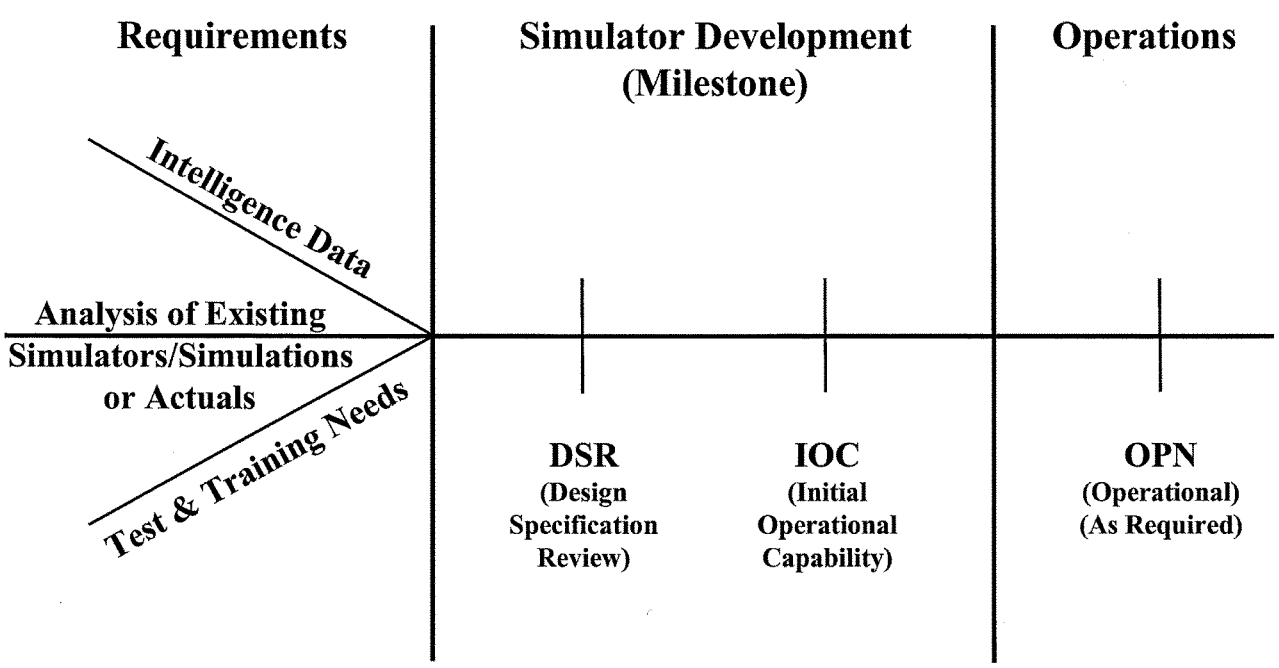

Figure Z–4. Validation events in the life cycle of threat simulators/simulations

(3) A periodic review is conducted on all legacy simulators/simulations to determine the need for an Operational (OPN) Validation. An Operational Validation is required on all threat systems/simulations after major modifications, significant changes to the intelligence data, or a significant change/degradation to the simulator/simulation to document their continued capability to represent threat systems as described by current intelligence estimates. The IOC VR will recommend critical parameters and intervals for OPN reviews. The VWG chairman will review the recommended intervals as well as the critical parameters to be considered. OPN validations consist of comparison and analysis of simulator/simulation performance, configuration, and fidelity to current threat estimates. Actual simulator measurements and/or simulation-generated data will be used in OPN validations but only for the critical parameters. The simulator/simulation/target MATDEV representatives, in coordination with the OPN VWG, may be required to designate/select the critical parameters if they have not previously been identified. For those systems, the first OPN VR may require a more extensive critical parameter list and other descriptive data to adequately establish the baseline information normally found in an IOC VR.

c. The general validation process requires the design, engineering and technical limitations of the threat system/simulation and its projected use be reviewed. To accomplish this review, the combined expertise of the intelligence community, the target or threat simulator/simulation developer, developmental and operational testers is required. Accordingly, a VWG composed of representatives from the above organizations will constitute the primary Army validation organization.

(1) During the engineering and technical analysis process, the design, engineering and technical characteristics and capabilities of a threat simulator/simulation (as outlined in the SD or other related document) are analyzed and compared to current DIA approved threat intelligence (as outlined in the TSP or other threat related document) for the related threat system. The results of this process will be documented in section V, and summarized in section VI, of the VR.

(2) An operational analysis is also accomplished by the VWG. It compares the capabilities and limitations of the threat simulator/simulation as found during the design, engineering and technical analysis, with the threat's operational characteristics to ascertain its performance capabilities. Details from this operational analysis will also be discussed in section V and summarized in section VI of the VR.

d. Validation Working Groups (VWGs) will evaluate and report on threat targets or threat simulators/simulations at the required points in the life cycle identified in paragraph Z–10*b* (Validation Requirements).

(1) A VWG will be established and chartered for each target or threat simulator/simulation, and usually for each validation requirement. TEMA will charter VWGs based on schedules provided by PM ITTS. The charter will establish TEMA as chairman and designate the organizations to participate in the VWG.

(2) Generally, VWGs are composed of representatives from the responsible user, IPC, PM ITTS, and the simulator/

simulation or target development organizations. Representatives from the following organizations will participate in VWGs as indicated:

(a) Mandatory members include representatives from ATEC, the appropriate IPC for the system(s) involved, U.S. Army Materiel Systems Analysis Agency (AMSAA), PM ITTS, Department of the Army Deputy Chief of Staff G–2, and the Threat Simulator or Target developer (if other than PM ITTS).

(b) Additional members as required include U.S. Army Research Laboratory (USARL), U.S. Army Materiel Command Research Development and Engineering Centers (RDECs), TRADOC, PEO/PM (appropriate blue systems), other Army organizations, and other DOD representatives as deemed necessary by the VWG chair. General functional areas and organizations, as well as general membership are shown in figure Z–5. The events involved in validation are illustrated in figure Z–6. The functions and responsibilities of the VWG are discussed below.

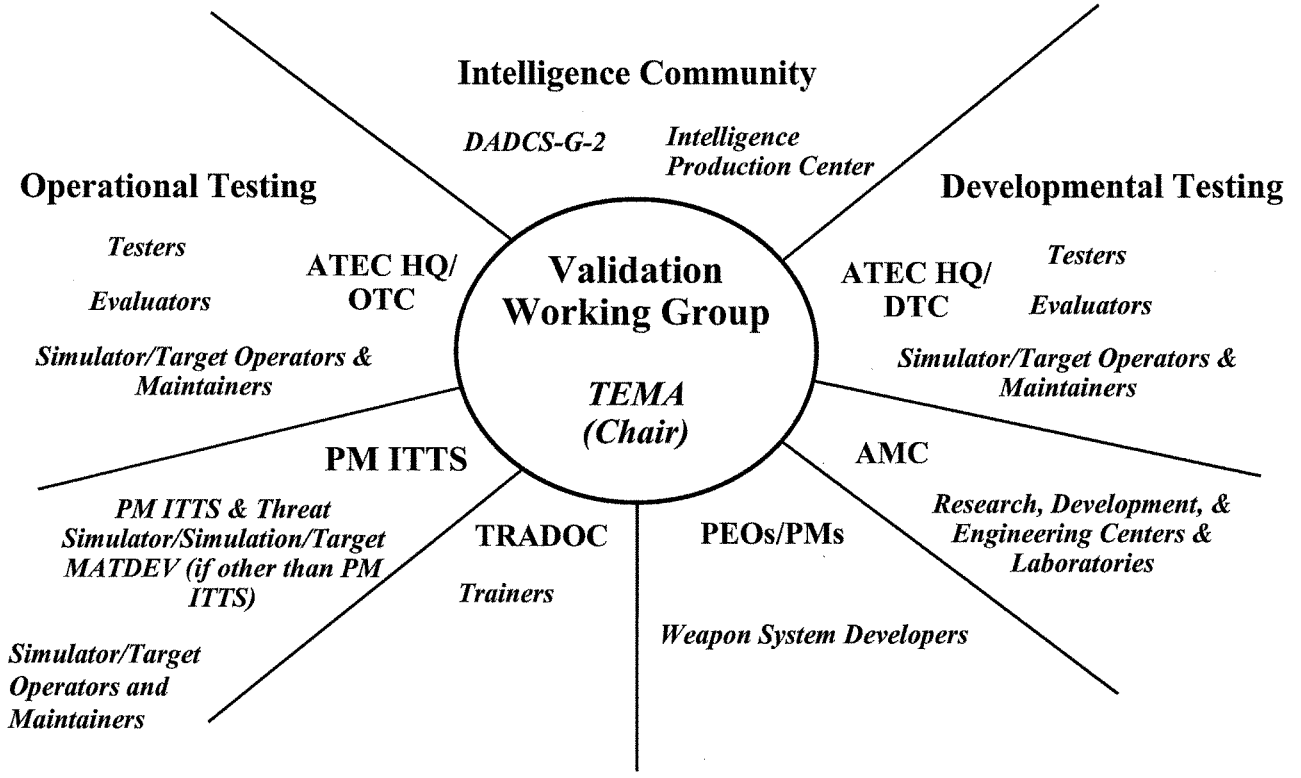

Figure Z–5. Validation Working Group membership pool

(c) The DOT&E approved standard validation criteria cover a broad spectrum of parameters that describe threat systems. Upon establishment of a VWG, the threat system MATDEV representative, in coordination with the IPC representative, will tailor a set of standard validation criteria for use in validating the simulator/simulation in question. The proposed criteria will be drawn from approved DOT&E standard validation criteria and may be augmented if required. The VWG will ensure that the standard validation criteria (parametric listings) describing threat equipment are used for both the TSP and the SD. If DOT&E approved standard validation criteria are not available, the simulator/ simulation or target MATDEV, in coordination with the IPC, will develop a proposed set of criteria to be used for the validation. The coordinated proposed validation criteria will be forwarded to the VWG chairman for approval, and to DOT&E for information. The same standard criteria will be used for DSR and IOC validations.

(d) Design, engineering, technical, and operational analyses will be conducted by the VWG.

(e) Information will be documented in a Validation Report.

(f) VWG will submit the required VR for approval (at IOC) or for notification, information, and retention (at OPN) to DOT&E. The VR should be forwarded using a letter of transmittal. The VR parametric data format and simulation summary reports are illustrated in tables Z–2 and Z–3, respectively (sample only; no actual data shown).

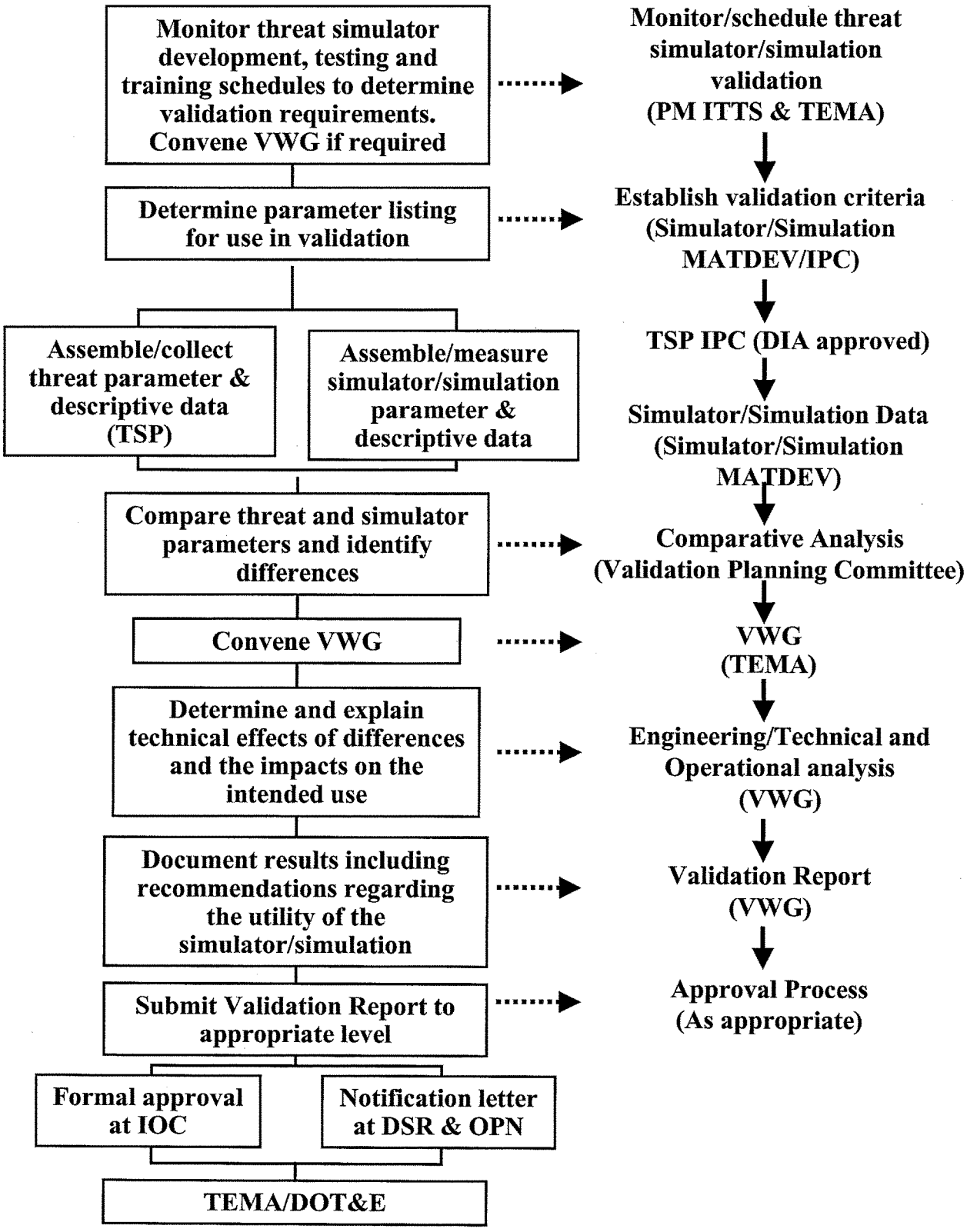

Figure Z–6. Validation event cycle

Table Z–2
Sample Simulator/Simulation Validation Report parametric data format

CROSSBOW #	Subsystem/ parameter	Units	DIA threat estimate low-most-high	Simulator/ Simulation target value	Remarks	Deltas	Impact
J1.1	RF communica-tions	Yes/No	No	No			
D2.223.5	RF power out	Watts	5	3	Rem2	2	D1
R4.234.7	Antenna length	Meters	1: 1.5	Nap		Yes	F4
			2: 4	Nap		Yes	F4
			3: 3	Nap		Yes	F4
P3.3	Polarization	Text	Vertical	Vertical			
F1.2.3.5	Antenna type	Text	Whip	Log period		Yes	A3
C1.0	Number of bands	Integer	1	1			
P3.4.5	Radiated power	dBW	50 to 60	70		10	D3

Table Z–3
Sample Simulation Summary Report

Entity	Function	Confidence	Comments
Target Acquisition Radar (TAR)	Detection	No clutter - HIGH Clutter - MEDIUM	Simulation of the TAR operating in a no-clutter environment produces results consistent with FME.
TAR	Detection	Clutter - MEDIUM	No data are available to validate simulation results for a clutter environment.
TAR	Mode Logic	High	Consistent with FME findings and intelligence information
	Waveform Logic	High	Consistent with FME findings and intelligence information
Target Tracking Radar (TTR)	Track Accuracy	No Clutter - MEDIUM	No actual test data available, however, track errors are lower than engineering analysis assessments
TTR	Waveform Usage	HIGH	Consistent with FME findings and intelligence information. TTR wobulation mode is not modeled due to limitations in the JMASS signal packet.
Weapon Controller	Launch solution	HIGH	Consistent with FME findings, except that the missile launch solution does not observe 300 m/s launch limit on outbound targets.

(g) Threat simulators/simulations developed and fielded prior to implementation of DOD threat validation procedures were not subject to the developmental validation process, such as the DSR and IOC validations. They are, however, subject to the provisions for OPN validation. For those systems, the MATDEV, in conjunction with the user or the owning organization, and the responsible IPC will determine the OPN validation cycle. The resulting schedule will be forwarded to TEMA, who will then establish and notify members of the OPN VWG. If critical parameters for OPN validations have not previously been developed, the MATDEV, in conjunction with the user or the owning organization, and the appropriate IPC will develop a list of critical parameters and forward them to the VWG chairman for approval. Any unresolved issues regarding OPN validations will be sent to TEMA for resolution.

(h) The VWG will determine an appropriate location for the conduct of the OPN validation. The VWG will base its decision on a thorough review of changes in the threat and other pertinent factors that may impact the amount of effort involved in conducting the OPN validation. The VWG will then select the most convenient, least disruptive (to testing), and least expensive location suitable for the conduct of the OPN validation measurements.

e. The VWG Planning Committee assists the VWG in its mission to ensure all threat systems are validated prior to accreditation and use. In its role as chair, PM ITTS will—

(1) Chair a minimum of two planning meetings per year, alternating with the semiannual DA VWG meetings. Additional meetings may be necessary to support VWG activity and assist TEMA in the execution of its Army Threat Systems/Simulation Validation responsibilities. Typically meetings are scheduled as follows:

— VWG Planning Meeting - April
— VWG - Late May
— VWG Planning Meeting - August
— VWG - Early November
— VWG - Planning Meeting - December
— VWG - March

(2) Solicit attendance to the Planning Committee meetings as warranted. Members of the planning committee will normally be representatives of the core VWG membership. A representative from TEMA will attend these meetings to provide program guidance and present the DA perspective relative to agenda items and the ensuing discussions pertaining thereto.

(3) Conduct planning meetings to—

(a) Address VR issues prior to consideration by the VWG.

(b) Develop validation goals and objectives based on known test events requiring validated threat assets.

(c) Develop, and annually publish, a validation schedule with required updates as warranted throughout the year to ensure currency and accuracy.

(d) Ensure that the AMC ATSMP is crossed-walked with the validation schedule to ensure accuracy.Review accreditation schedules to ensure planned system validations are being conducted in sufficient time to provide necessary data in support of ATEC's threat system accreditation program.Annually canvass the acquisition and T&E communities to further identify threat system validation requirements.

(e) Provide quarterly validation schedule change updates to the VWG membership in conjunction with the preplanned meetings cited above. If these meetings are not held, a quarterly updated change report, if required, will be forwarded to the VWG membership.

(4) Provide recommendations to TEMA on validation waiver requests.

(5) Provide planning committee meeting minutes to TEMA within 30 days after the conclusion of the meeting.

(6) Participate in OSD VWG forums as required.

f. Specific Validation Procedures. It is essential to keep the validation process as simplified and non time-consuming as possible without degrading the quality of the reports. Content rather than appearance should be the primary focus.

(1) Table Z–4 outlines the procedures for systems undergoing DSR and IOC validations.

Table Z–4
Threat Simulator/Simulation DSR and IOC Validation Report

Item	Procedures
1	PM ITTS monitors/coordinates TSP requirements and validation schedules and submits data to TEMA.
2	TEMA coordinates/transmits TSP requirements with HQDA (DCS, G–2) and TSIWG.
3	TEMA charters a VWG. If required, a planning and coordination meeting will be convened to establish the validation parameters listing.
4	The appropriate Intelligence Production Center provides or produces the TSP and forwards it to the VWG chairman.
5	Simulator developer produces the system description document. Simulation developer produces a Functional Requirements Document (FRD) and validation plan.
6	Under the direction of the VWG chairman, the MATDEV produces a document listing the validation parameters, threat values, simulator values or simulation-generated data, and the delta between the threat and simulator or simulation-generated values.
7	VWG analyzes the design, engineering and technical implications regarding the deltas of the capabilities of the simulator or simulation.

Table Z–4
Threat Simulator/Simulation DSR and IOC Validation Report—Continued

Item	Procedures
8	TEMA or a designee convenes and chairs the VWG, which will normally be scheduled as 1-day meetings. The analysis is reviewed and final coordination completed. The VR is signed by all VWG members and when appropriate, forwarded to the TSIWG chairman for approval.

Notes:

[1] The VR contains the following—Validation and simulator/simulation parametric values, threat parametric values, and the parametric deltas between the threat and the simulator/simulation. Analysis outlining the design, engineering and technical impacts of the parametric deltas between the threat and the simulator or simulation regarding the actual operation of the simulator. Analysis outlining the impacts on testing of the parametric deltas. Cover letter forwarding the report with the results of the analysis and recommendations concerning continued development/additional data requirements and/or modifications. IOC VRs contain critical parameters and time intervals between operational validations.

Table Z–5
Operational validation process

Item	Threat Simulator/Simulation Operational Validation Process
1	PM ITTS monitors/coordinates operational validation schedules and provides to TEMA. If not previously designated, PM ITTS, in coordination with the simulator/simulation owner, and the appropriate Intelligence Production Center, will recommend to TEMA critical parameters and schedules for use in operational validation.
2	TEMA coordinates operational validation requirements with HQDA (DCS, G–2) and the TSIWG.
3	The appropriate Intelligence Production Center approves the updated TSP developed by the MATDEV for the critical operational parameters only.
4	The owning organization will provide updated descriptive data and measurements of the critical operational parameters (that is, modified simulator data to match the modified TSP) to TEMA and PM ITTS.
5	TEMA/PM ITTS determines whether or not a full VR is required. This decision is based upon an analysis of both the updated threat and simulator data to determine if significant changes have occurred. If significant changes have not occurred, TEMA coordinates a statement to that effect with the VWG membership. This completes the operational validation process.
6	If significant changes have occurred, PM ITTS, in conjunction with TEMA, directs the conduct of an operational validation.
7	TEMA or a designated organization convenes and chairs the VWG. Based on actual measurements of the threat system's critical parameters, the VWG analyzes and compares the threat system performance, configuration, and fidelity to current threat estimates.
8	The results of the comparison and analysis are documented by the simulator/simulation owner and forwarded to TEMA.

Notes:

[1] Operational validations may be limited to one page of statements indicating no significant deltas exist between the critical parameters of the threat system and current threat estimates. This one page is attached to the last VR to serve as an updated operational validation.

(2) OPN validation procedures are designed for systems already fielded and are a modification of the general validation procedures. Table Z–5 outlines the procedures for OPN validation. The operational validation is concerned only with the critical parameters. The owning organization will provide to TEMA updated simulator/simulation/target data and updated threat DIA approved intelligence from the IPC. TEMA will determine if a full operational validation report is required. The decision will be based on an analysis of both the updated threat and simulator/simulation/target data to determine if significant changes have taken place that concern the critical parameters. If it is determined that significant changes have not taken place, TEMA will coordinate with the VWG members to sign off on a statement to that fact. The statement is attached to the front of the most recent VWG report and serves as an updated operational validation. If significant changes have taken place, the owning organization will produce an abbreviated VR (limited to the critical parameters) and the general validation procedures will be followed.

(3) Special procedures for validation of Programmable Threat Simulators (PTS). Validation of PTS will be in accordance with a three-phased process negating the need for costly, repetitive validations. The intent is to reduce the cost associated with validating PTS, without compromising the validity of the threat representation utilized in testing. The three phases are—

(a) Phase I—Establish Limits and Diversity Characteristics. The first step is to establish a list of critical validation parameters for the specific PTS based upon the critical threat parameters. The Army VWG then convenes to review and approve the list of critical validation parameters for the PTS. Once approved, the limits and diversity characteristics of the PTS critical parameters will be established through testing.

(b) Phase II—Demonstrate Programmability. The second phase is to demonstrate the programmability of the PTS. A small sample of threat systems (3 to 5) will be chosen to demonstrate the capability of the PTS to replicate various

aspects of the selected threat systems. The sample size should be proportional to the complexity and diversity of the PTS, with threat systems chosen to demonstrate the limits of the PTS wherever possible. The PTS will be configured to replicate each threat system in the sample group. Parametric measurements will be taken and the resulting data compared to the DIA approved intelligence data for the corresponding threat system. Any differences that exist between the simulator data and the threat data will be analyzed to determine potential impacts or limitations on simulator usage. These measurements should be conducted in conjunction with the measurements required in Phase I.

(c) Phase III—Documentation and Approval. The final phase of the process is the documentation and approval phase. Data and information gathered in the first two phases will be compiled in a PTS VR. The format for this report is the same as used for other VR, although some changes may be required based on the individual PTS. While a standardized format is desired, the focus of the report will be the presentation of the relevant data and information, including a comparison matrix (Standard Validation Criteria Tables) with identified differences and potential impacts discussed. Once a Draft PTS VR has been completed, it will be presented to the Army VWG members for review and approval in accordance with AR 73–1. After the Army VWG has approved the PTS VR, the VWG will recommend that the PTS be validated as a threat simulator for all threat systems whose critical parameter values fall within those of the PTS performance parameters. As with all threat simulator reports, TEMA's Director will approve the PTS VR and forward it to DOT&E for final approval as required. Once approved, the PTS is authorized for use in support of testing until the next scheduled operational validation review.

(4) Foreign materiel validation procedures are a modification of the threat simulator/simulation/target validation process. Foreign systems are generally exploited or baselined by the IPC. Baseline or exploitation data will be made available to the VWG by the IPC. When available, the IPC exploitation report will be used by the VWG as the basis for validation of the exploited system. For actual systems where no intelligence data exist, the measured data will be approved by the IPC and used to establish the threat baseline. Certification is designed simply to verify the authenticity of the threat and to document any shortcomings, degradations, or modifications to the system. Certification Reports for actual systems may be used in lieu of VRs for the accreditation process.

(a) If an actual threat system is to be used as a surrogate for another threat, (for example, a T–72 tank used to represent a T–80 tank), the surrogate will be subject to the validation and accreditation procedures outlined in this document.

(b) Actual threat systems will be considered validated after completing the certification procedures outlined below.

— The MATDEV will coordinate the development of a list of critical parameters necessary to adequately identify and describe the threat system undergoing certification. As a minimum, concurrence from the appropriate IPC and user will be received. To the extent possible, the parameter listing should be in DOT&E's authorized format to facilitate documenting the configuration of the actual threat system.
— The MATDEV will obtain DIA-approved system specification data from the appropriate IPC for the type system undergoing certification. The MATDEV will then extract the necessary threat values for the certification parameter listing previously developed for the system. Additionally, the MATDEV will extract sufficient descriptive data to provide a short narrative description and overview of the system and its capabilities. Where possible, information concerning any variants of the system should be included (for example, how an A model differs from a B model). All data sources will be properly documented.
— PM ITTS will inspect the actual threat system undergoing certification and verify that the parametric data values obtained from DIA sources are present on the actual equipment. Any differences noted will be documented. Draft impact statements will be prepared reflecting any potential test or training limitations caused by the deltas. Parameters that may not have been addressed during the validation process and are considered critical to a particular tester will be measured and compared to DIA approved intelligence data during the accreditation process for that test.
— The completed certification report (parameter listing, descriptive data, and impact statements) will be staffed with the appropriate IPC and user then forwarded to TEMA for approval. If necessary, a VWG meeting will be held to finalize the comments. A copy of the certification report will also be forwarded to the TSIWG chairman for information purposes.
— Certification reports will be maintained as part of the maintenance and usage records of the equipment. Organizations owning actual threat systems are responsible for ensuring that any changes in the actual threat system configurations are properly documented. The MATDEV, in conjunction with the owning organization and the responsible IPC, will periodically review the changes and make recommendations to TEMA regarding the need for recertification or possibly an OPN validation.

Z–11. Validation of targets

a. Overview of the general target validation process.

(1) Target validation will be accomplished and documented by a VWG. Due to the specificity and uniqueness associated with signature development, many of the generic aspects of validation are not applicable. The procedures for validation and accreditation of targets will be modified as outlined in this section.

(2) Target developments generally fall into two broad categories. First, there are generic targets used to represent a wide range of similar type threats. An example of this type target would be the MQM 107 used to represent subsonic fixed wing aircraft. Second, there are targets (which could include actual systems) designed to represent a single threat, with signature replication to meet specific testing milestones. For each of these cases, the validation can be streamlined by making modifications to the procedures outlined for threat simulator/simulation validation.

(3) For all targets projected for use in training or testing that will support a milestone decision, validation will occur at DSR and IOC. OPN validations are required periodically throughout the life cycle or after major modifications that affect target fidelity or alter the signature of the target, such as the addition of reactive armor or an engine upgrade. This is normally required only for targets representing a specific threat.

(4) All target VRs will be forwarded to TEMA for approval. DSR validation will be completed during target development and comply with the same procedures as identified above for threat simulators/simulations. IOC reports will be approved prior to a target being used to support a milestone decision review. The target MATDEV is responsible for funding validation.

b. The target validation process. The target validation process described in this section is shown in figure Z–7.

(1) Generic targets are defined as targets not designed to represent a specific threat. They are generally used to portray a family of threats such as fixed wing subsonic aircraft and rotary wing aircraft. These targets are often augmented with add-on kits to meet specific signature requirements for a given test. These types of targets will be baselined, which is simply the description, measurement, and documentation of the key parameters associated with the physical and operational characteristics of the target. Examples of the types of information documented include, but are not limited to, the length, width, weight, maximum speed, maximum altitude, and turning radius. The purpose of baselining is to provide sufficient data to the tester/developer so they can determine if the target will meet their general requirements. Separate appendices should be included in the baseline report to describe any augmentation kits that can be attached to the generic target. Generic target baseline reports will be prepared and approved by the target MATDEV and an information copy forwarded to the Director, TEMA. All comparisons of generic type targets to specific threats will occur during the accreditation process. Target accreditation will follow the accreditation procedures outlined for threat simulators/simulations.

(2) Threat specific targets will follow a modified threat simulator validation process as outlined below. As an exception, threat specific targets that do not portray electronic signature data (such as, only visual and performance characteristics) will be validated according to the threat simulator/simulation procedures described in paragraph Z–10 (validation of threat simulators/simulations). Infrared (IR), millimeter wave (MMW), seismic, and acoustic data are considered electronic. The MATDEV representative, in coordination with the IPC representative, will tailor a set of standard validation criteria for use in validating the threat in question. The proposed criteria will be drawn from approved DOT&E standard validation criteria and may be augmented if required. The VWG will ensure that the standard validation criteria (parametric listings) describing threat equipment, prepared from the listings approved by DOT&E, are used. If DOT&E approved standard validation criteria are not available, the MATDEV, in coordination with DOT&E and the IPC, will develop a proposed set of criteria to be used for the validation. The coordinated, proposed validation criteria will be forwarded to the VWG chairman for approval. The same standard validation criteria will be used for DSR and IOC validations.

(3) Signature data for threat specific targets will be validated as indicated below.

(a) The specific signature requirements for known tests will be collected.

(b) Signature parameter definitions will be developed by the supporting IPC.

(c) Threat signature data will be collected or developed by the supporting IPC in accordance with the developed parameter definitions and the approved test requirements. approved test requirements. The MATDEV will arrange for the appropriate organization to conduct the target signature measurements. The MATDEV and other members of the VWG will complete an engineering and technical analysis, comparing the target and threat signature data. Complete actual signature measurements are possible only at the IOC validation point. For DSR, the results of the engineering and technical analysis, along with any other relevant information will be evaluated. Maximum effort should be made to utilize advanced modeling and simulation techniques to predict signature replications. The results of the engineering and technical analysis will be documented in section V and section VI of the VR.

(d) Target signature data will be measured in accordance with the parameter definitions.

(e) The VWG will compare the capabilities and limitations of the target with its operational use to determine the target utility, complete the VR, and submit it to TEMA for approval.

(f) All future signature data requirements for the validated target will be reviewed, developed, and approved as part of the accreditation process.

(4) Actual foreign equipment utilized as targets should follow the procedures outlined in paragraph Z–10*f*(4). Any additional data required for training or testing should be documented as part of the accreditation process. Procedures outlined for threat simulator accreditation should be followed.

(5) Joint use targets will require approval by TEMA and DOT&E.

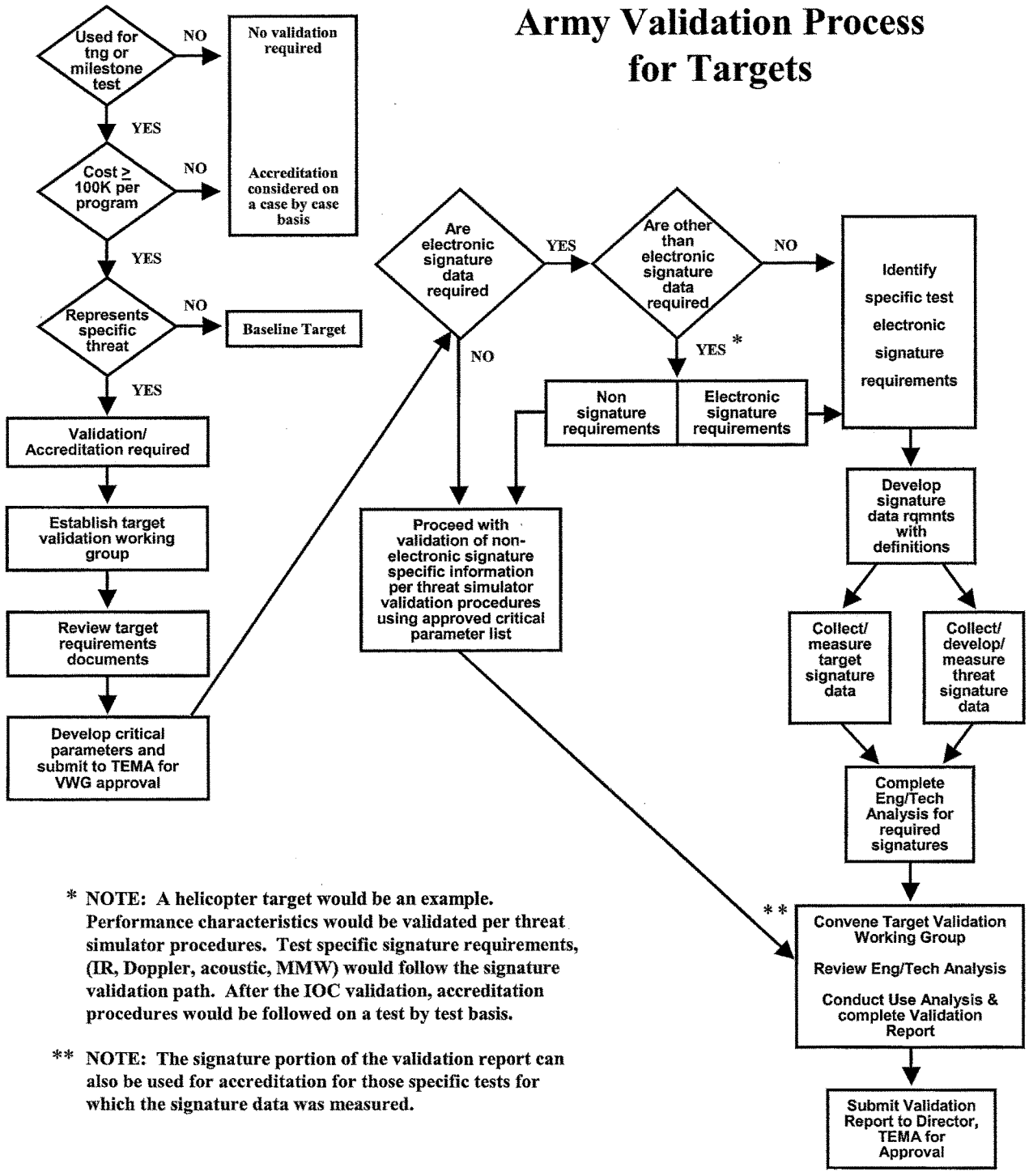

Figure Z–7. Army validation process for targets

Z–12. Accreditation

a. Accreditation is the process used to determine whether threat simulators/simulations, surrogates, actual threat systems, and targets are suitable for a specific test. The data requirements are compared to the latest intelligence and the capabilities of Army threat simulators/simulations and targets as shown in current VRs. In cases where VRs are not available, or where other constraints make validation unfeasible, waivers will be handled on an exception basis. All requests for exceptions/validation waivers will be forwarded to TEMA for approval. ATEC will not proceed to accredit threat systems for OT testing unless a waiver for validation has been approved by TEMA. Accreditation examines any parametric differences to determine their impacts on the test or training application. A complete validation of a threat system prior to accreditation/OT testing should provide sufficient documentation of the threat system's operational status, permitting analysts to quickly eliminate or include the threat system performance or its overall condition as a contributing factor to a failed test event by a system under test (SUT). To assist in projecting validation actions, ATEC will publish an annual accreditation schedule that is updated 6 months from publication to reflect cancelled or added test programs. The Accreditation Event Cycle is depicted in figure Z–8. General functional areas for organizations participating in accreditation are outlined in figure Z–9.

(1) Threat accreditation is essential for the following reasons:

(a) Any differences between a threat simulator/simulation/target and the corresponding actual threat system can distort representation of the threat. Even the differences accepted during development and validation can make the simulator/simulation or target incapable of adequately representing the threat for a specific test or training exercise.

(b) The intelligence concerning threat systems is dynamic. New intelligence can make a simulator/simulation or target inappropriate for a given test or training application.

(c) Threat simulators and targets experience deterioration and failures that can render them no longer threat representative. Models and simulations often require updates due to intelligence data, operating system or compiler changes. Accreditation decisions, therefore, must be based on current assessments of the performance of the simulators/simulations and targets.

(2) Accreditation for testing is accomplished under the auspices of the weapon system PEO/PM whose system is undergoing test and is documented in support of the weapon system T&E WIPT. Responsibilities for accreditation costs will be in accordance with AR 73–1. Threat simulator/simulation, target, and test usage requirements will be identified in sections 4 and 5 of Part V of the system TEMP. These paragraphs should include the number, type, and fidelity requirement, compare threat requirements, and note the shortfalls.

(3) Accreditation is required for any testing where the data will be used to support milestone decision reviews. For OT, the accreditation process complements the function of the Threat Coordinating Group (TCG) and T&E WIPT (to include the Threat subgroup) to improve test planning by specifically defining test resource requirements for the specific application in the OTP, which must be submitted for approval to the TSARC before test design and threat support planning can be fully documented. For all testing, TCG and accreditation affords an early opportunity for the weapons system MATDEV, evaluator, tester, and threat manager (TM)/Foreign Intelligence Officer (FIO) to coordinate respective test planning efforts.

(4) For OT, the process should be accomplished to allow timely inclusion of accredited threat simulator/simulation and target resource requirements in the final OTP for approval by the TSARC. TSARC policy requires at least a two-year lead-time between TSARC approval and first allocation of personnel and equipment from an external organization (see AR 15–38). An in-cycle OTP must be submitted to ATEC for review and staffing 9 months before its presentation to the TSARC.

b. Threat Accreditation Working Group (TAWG) membership and responsibilities are described as follows:

(1) TAWGs will be established under the auspices of the T&E WIPT by the PEO/PM whose weapon system is being tested. For all tests of ACAT I, ACAT II, or any other system on the OSD T&E oversight list ATEC will either chair or designate a TAWG chair. Records of DT and OT TAWGs should be maintained by the appropriate ATEC Support Team (AST) chair to ensure threat consistency throughout testing. For ACAT III programs not on the OSD oversight list, ATEC will designate the TAWG chair with the assistance of the AST chair. The chairman of the T&E WIPT for each program will coordinate with the ATEC Threat Coordination Office to have a TAWG chairman appointed; subsequently, the TAWG membership will then be notified that the TAWG is established and its chairman appointed. Future TAWG direction will come from the TAWG chairman. A TAWG determines if the simulators/simulations and targets proposed for a specific test have the capability to represent the relevant threat characteristics needed during that test. All parties to the test planning process, particularly the threat proponents, must be aware of the requirement to accredit targets and threat simulators/simulations and share responsibility to notify the T&E WIPT/AST chairs, as early as possible, of the need to establish a TAWG. All parties to the test planning process also must be aware of the requirement that all threat-specific targets, generic targets with threat-specific components, and all threat simulators/simulations have a validation requirement and must notify the ATEC Threat Coordination Office through the T&E WIPT/AST chairs, as early as possible.

(2) TAWGs will be composed of representatives from the responsible PM, PEO, T&E WIPT, intelligence, threat simulator, and target developmental or operational organizations. Representatives of the following organizations will participate as determined by the chair, DCS, G–2/TISO, TRADOC (designated threat manager or TRADOC ODCS, G–2), ATEC (tester and evaluator), AMC, AMSAA, appropriate IPC, MATDEV for threat simulator or target, ARL, appropriate PM/PEO, and others as required.

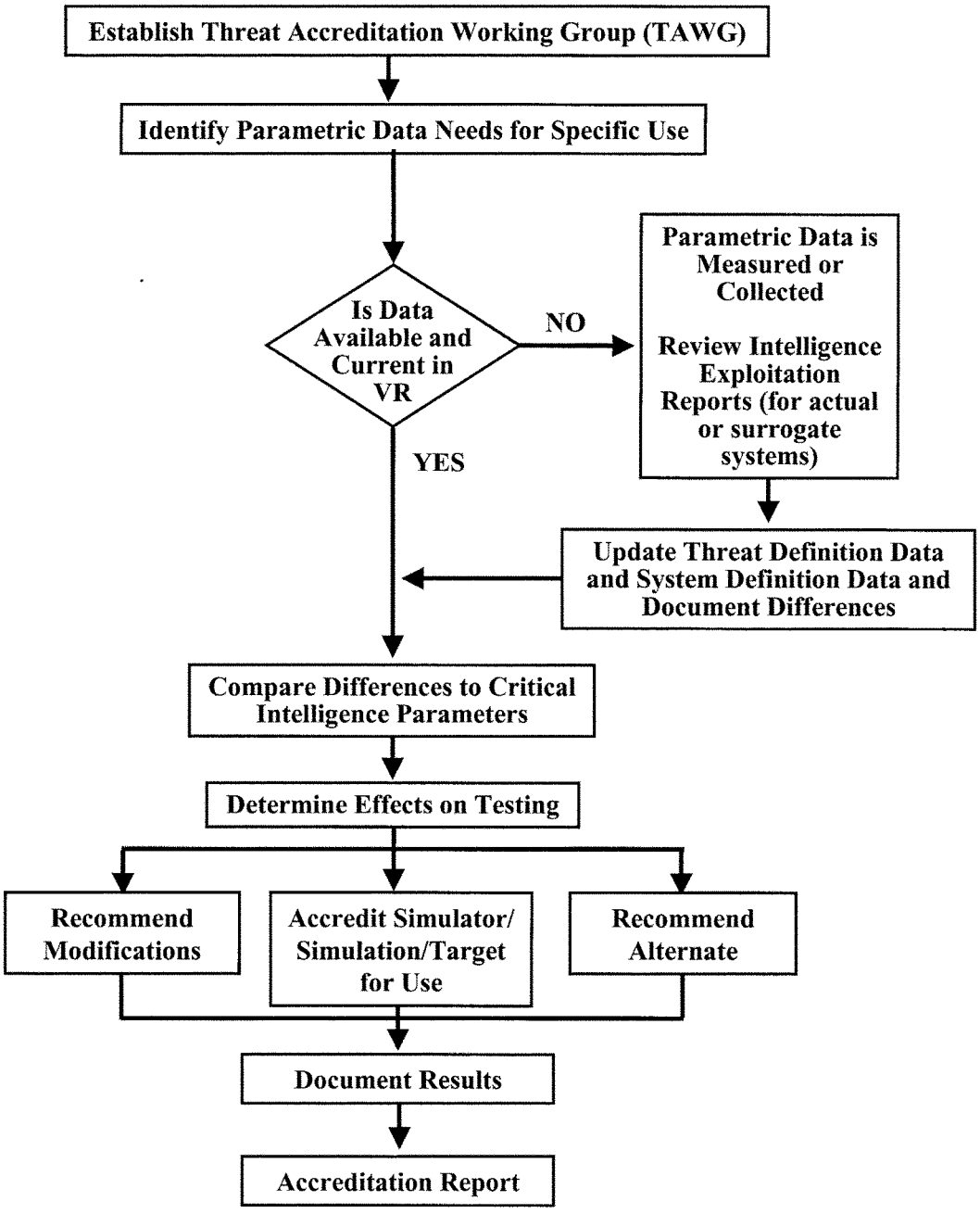

Figure Z–8. Accreditation event cycle

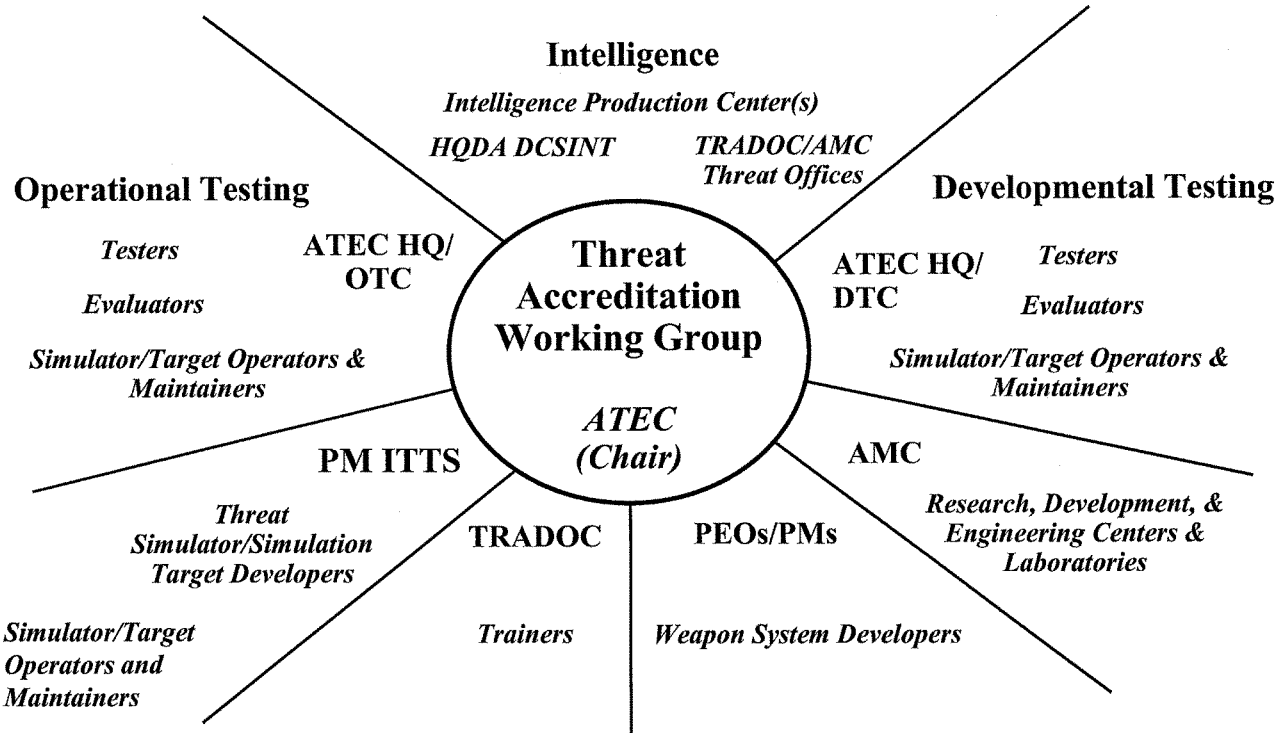

Figure Z–9. Threat Accreditation Working Group membership pool

(3) The TAWG will review the technical requirements for the threat simulators and targets, and the simulator/simulation and target validation data, to determine the capability of the simulator/simulation and target to represent relevant system characteristics for the test under consideration.

(4) The TAWG will document, via an accreditation report to the T&E WIPT, the suitability of the individual threat simulators/simulations and targets for use in support of the specified test under consideration. A letter of transmittal (fig Z–10) will be used to forward the report to the T&E WIPT chair. Where more than one threat simulator/simulation or target is being accredited for the same test, the findings regarding each may be combined into a single report and forwarded to the T&E WIPT chair using the same transmittal letter.

(5) Due to the diverse nature of issues that may be addressed during accreditation, a standard report format is not provided. The content of the transmittal letter serves as a guide for what should be contained in the accreditation report.

(6) The following procedures should be followed by the TAWG:

(a) TAWG members first identify specific parametric data needs to satisfy the Critical Operational Issues and Criteria (COIC) for the planned testing. The threat simulator/simulation/target developer, or simulator/simulation/target owning organization, for systems already fielded, will verify that all parametric data provided in the VR are current. Any required data not included in the VR must be collected or measured as part of the accreditation process. The Threat Integration Staff Officer (TISO) will coordinate the verification and update of applicable parameters (characteristics and capabilities) of the threat system. The threat simulator/simulation and target developer, or simulator/simulation/target owning organization, for systems already fielded, will verify or update the same parameters of the corresponding threat simulator/simulation or target. The TAWG documents the differences between the simulator/simulation or target and the threat in a preliminary accreditation report.

(b) For generic targets or targets not previously subjected to the validation process, which will be used to represent a specific threat for a given test, the responsible MATDEV must provide the TISO with documented system parameters for comparison with the intelligence on the corresponding threat system. These parameters should consist of only those necessary to support the particular test or training scenario for which the system is to be used. For actual threat systems and surrogate systems, the TAWG IPC member may use intelligence exploitation, validation, certification, or baseline reports. The parametric on the threat system and those of the corresponding threat simulator/simulation and target, and the differences between them, will be formally documented by the TAWG in the accreditation report.

[CLASSIFICATION]

TO [CHAIRMAN, APPROPRIATE T&E WIPT]
SUBJECT: [Name of Threat Simulator / Target Accreditation Report]

1. Provide the title of the threat simulator/simulation(s) or target(s) being accredited.
2. Identify the applicable test event by title and Test Schedule and Review Committee (TSARC) number.
3. Identify the working group charter by issuing headquarters, title and date. Append a list of the working group membership.
4. Identify, by title and date, the DIA Threat Estimate used for the report preparation.
5. Parameters are only referenced in the transmittal letter, with details contained in the subject report. The report should include CIP as defined in AR 381-11, user required critical operational characteristics and capabilities as defined in the requirement document, and applicable Standard Validation Criteria.
6. Data collection/analysis is summarized in the transmittal letter, with details contained in the subject report. The report should itemize any data collection/analyses conducted (by whom, when, and where) to determine the suitability of the simulator or target to support the critical issues and criteria of the test being supported.
7. A brief summary of the major results of the data collection/analysis should be in the transmittal letter. The full report should provide full results, plus identify differences and the effect on simulator/target capability.
8. Only differences with a significant impact on testing or training need to be mentioned in the transmittal letter, with all remaining differences discussed in the subject report.

SIGNATURES: All appointed members of the TAWG

[CLASSIFICATION]

Figure Z–10. Accreditation Report letter of transmittal

(c) Differences between the threat simulator/simulation or target and the intelligence concerning the capabilities of the relevant threat system must be assessed against the critical intelligence parameters (CIPs) to determine whether the performance characteristics representing the threat are within the CIPs established by the system program manager. Differences, particularly those that breach CIP thresholds, that cannot be accommodated or offset in test planning are defined and assessed to justify modification of the simulator/simulation or target, or acquisition of alternate simulators of targets. Differences assessed to breach CIP thresholds and impact on the effectiveness, survivability, and cost of the U.S. systems under development must be reported to the T&E WIPT with recommendations.

(d) Collectively, the TAWG assesses the differences between the threat simulator/simulation or target and the intelligence concerning the capabilities of relevant threat system in the context of test data requirements to determine the impacts on the test, including test limitations. These differences are then documented in the accreditation report.

Section III
Roles

Z–13. Instrumentation requirements role

a. Army Test and Evaluation Command—

(1) Provides identification of, documentation for, and adjustment to requirements for Instrumentation, Target, and Threat Simulator Program plan processes.

(2) Provides empowered representatives to participate on appropriate Working Groups as required.

(3) Provides coordinated ATEC priorities, project descriptions, and financial estimates on major instrumentation requirements.

(4) Provides coordination and support of all ATEC ITTS programs throughout program development plans and funding cycles.

(5) Executes sustaining instrumentation programs.

(6) Biannually sponsors the ATEC Test Instrumentation Conference (ATIC). Participants include ATEC HQ, ATEC subordinate command, OSD, PM ITTS, and other invited agencies as it pertains to the focus topics of each conference.

b. Army Space and Missile Defense Command—

(1) Provides empowered representatives to participate on appropriate WGs as required.

(2) Provides coordination and support of all USASMDC major instrumentation programs throughout the program development plans and funding cycles.

(3) Executes sustaining instrumentation programs.

c. Program Manager for ITTS—

(1) Develops, Acquires, fields, operates and maintains, and provides life cycle management of Army targets, threat simulators/simulations, and selected major test instrumentation except those designated by regulation to other Army agencies, such as SMDC.

(2) Provides empowered representative participation to ATEC's instrumentation, targets, and threat simulator/ simulation requirements processes.

(3) Gathers and integrates Army test requirements into a shared, Army-wide approach to ITTS investment.

(4) Provides coordination and contact with ATEC regarding all ATEC instrumentation, targets, and threat simulator/ simulation requirements and the execution of projects against those requirements.

(5) Establishes working groups for each major instrumentation, target and threat simulator/simulation program. Participants will include, PM ITTS, TEMA, ATEC HQ, and appropriate representation from ATEC subordinate commands as required and determined by ATEC HQ.

d. Army Test and Evaluation Command and Program Manager for ITTS jointly—

(1) Ensures that all ITTS investments in both commands are regularly reviewed and updated as cost, schedule, or performance requirements change or as funding available for execution changes.

(2) Hosts, setting agendas, and attending a semiannual review during which the status of all major instrumentation, targets and threat projects under PM ITTS and under ATEC execution will be reviewed.

(3) Presents the authenticated prioritized listing of ITTS programs to TEMA as a coordinated agreement

Z–14. Validation of threat simulators/simulations role

a. Deputy Under Secretary of the Army (Operations Research) provides overall DA-level program direction, guidance, review, and approval authority.

b. Test and Evaluation Management Agency—

(1) Approves and transmits copies of VRs with appropriate forwarding or notification letters to the DOT&E as required.

(2) When required, coordinates Air Force and Navy participation in the validation process.

(3) Prioritizes and coordinates all Army requests for threat data in support of validation.

(4) Chairs all DA level VWGs. Charters all other VWGs as warranted and appoints the chairman.

c. Training and Doctrine Command—

(1) Identifies and documents threat simulator and target requirements to support combat development efforts.

(2) Participates in VWGs as required.

d. PEO STRI—

(1) Identifies and documents threat simulator and target requirements to support testing and simulator materiel developmental efforts.

(2) Participates in VWGs as required

e. Army Test and Evaluation Command—

(1) Identifies, prioritizes, and documents threat simulator/simulation and target requirements to support testing.

(2) Participates in VWGs and validation planning meetings as required and formally disseminates information identified in (a) above.

(3) Participates in PEO STRI meetings as warranted

f. Intelligence Production Centers (as appropriate for the system being validated; coordination with Air Force or Navy channels will be accomplished as required)—

(1) Prepares TSPs as tasked by DIA, and provides them to the threat system MATDEV.

(2) Participates in VWGs.

(3) In coordination with the simulator or target MATDEV, develops a set of validation criteria.

(4) Provides exploitation baseline data for actual threat systems.

g. Program Manager for ITTS—

(1) Maintains an information and suspense file on all validation activities assigned by TEMA.

(2) Notifies TEMA when DSR, IOC, and Operational validations are due so that VWGs can be established.

(3) Develops, in coordination with the appropriate IPC, a proposed set of validation criteria.

(4) Participates in VWGs as required. Chairs the validation planning meetings. In this forum or through independent

review, ensures validation report soundness and compliance with overall intent of the validation process prior to initial staffing with core VWG members.

(5) Coordinates measurements of threat simulator and target parameters as required for comparison to the current DIA approved IPC estimates for the threat system.

(6) Develops a complete system description containing complete narrative, pictorial, and parametric description of simulator or target for comparison with the TSP. As required, serve as a technical consultant on VWGs.

(7) Prepares certification reports as required.

(8) Provides system description and data required for section IV and appendix A of DSR and IOC VRs.

(9) Funds validation efforts for which they are the designated MATDEV.

(10) Conducts measurements of threat simulator/simulation and target parameters required for OPN validations.

(11) Notifies TEMA when OPN validations are due so that VWGs can be established.

(12) In the absence of IOC VWG approved critical parameters, develops a proposed set of OPN validation criteria in coordination with the simulator system MATDEV and the appropriate IPC.

(13) Notifies TEMA of the need for Threat Support Packages.

(14) For owned systems undergoing OPN Validation, develops an updated system description containing complete narrative, pictorial, and parametric description of simulator for comparison with the TSP. Forwards updated system descriptions along with updated TSP data from the IPC to TEMA.

(15) Provides a system description and data required for section IV and appendix A of the OPN Validation Report.

(16) Funds OPN validations for owned systems.

h. Program Executive Officer/Program Manager—

(1) Identifies and documents in the development system's TEMP threat simulator and target requirements to support simulator materiel development efforts.

(2) Participates in VWGs as required.

Z–15. Accreditation of threat simulators/simulations, surrogates, actuals and targets roles

a. Department of the Army Deputy Chief of Staff, G–2—

(1) Maintains, reviews, and validates CIPs that affect the effectiveness, survivability, or security of U.S. systems.

(2) Designates TISOs for ACAT I, ACAT II, and other OSD T&E oversight systems.

(3) Coordinates and reviews threat support throughout the life cycle of developmental systems.

(4) Chairs TCGs for ACAT I and II programs and all programs on the OSD Oversight List in accordance with AR 381–11.

(5) Participates in T&E WIPTs, TCGs, and TAWGs as appropriate.

b. Test and Evaluation Management Agency coordinates with the HQDA DCS, G–2 for the integration of Army-approved threat in test programs, including DT, OT, or FDT/E, and JT&E.

c. Training and Doctrine Command—

(1) Provides COIC/Additional Operational Issues and Criteria for use by the TAWG.

(2) Provides the Threat TSP.

(3) Chairs the TCG for all ACAT III programs not on the OSD Oversight List, in accordance with AR 381–11.

d. PEO STRI—

(1) Participates in T&E WIPTs, TCGs and TAWGs as required.

(2) Develops the Threat TSP for DT if Threat Force operations are to be represented.

(3) Provides target and threat simulator technical performance data for use by the TAWG in assessing threat simulator and target suitability and adequacy.

(4) Measures threat simulators as required to ensure availability and accuracy of system data for accreditation.

e. Army Test and Evaluation Command—

(1) Coordinates test planning with the appropriate threat approval authority (see AR 381–11) to define the conditions and environment of both DT and OT to ensure that an appropriate battlefield environment will be portrayed.

(2) Participates in T&E WIPTs, TCGs, and chairs TAWGs for both DT and OT.

(3) Provides test concept and test design to the TCG and TAWG for their use in assessing threat simulator and target suitability and adequacy.

(4) For owned systems, provide target and threat simulator/simulation technical and performance data for use by the TAWG in assessing threat simulator and target suitability and adequacy.

f. Program Manager for ITTS (or MATDEV)—

(1) Provides the current VR for use by the TAWG in assessing threat simulator/simulation and target suitability and adequacy.

(2) For systems in development, provides target and threat simulator/simulation technical and performance data for use by the TAWG in assessing threat simulator/simulation and target suitability and adequacy.

(3) Measures threat simulator/simulation and target parameters as required for systems in development to ensure availability and accuracy of data for accreditation.

(4) Participates in TAWGs.

g. Intelligence Production Center (as appropriate for the threat systems undergoing accreditation)—

(1) Participates in T&E IPT WIPT, TCGs, and TAWGs are required to explain threat capabilities and limitations. The IPC representative should be an expert on the threat system being simulated.

(2) Participates in the TAWG to refine threat simulator/simulation/target requirements and assess the impacts of difference between the simulator/simulation/target and the threat.

(3) Provides threat assessments and documentation to the TAWG.

(4) Updates or verifies threat data as required.

h. Program executive officer/Program manager (as appropriate for weapon system undergoing test)—

(1) Establishes TAWGs under the auspices of the T&E WIPT.

(2) Participates in TAWGs as appropriate.

(3) Requests waivers for systems that have not undergone validation.